HP ProtectTools

お使いになる前に

Bluetooth は、その所有者が所有する商標であり、使用許諾に基づいて Hewlett-Packard Company が使用しています。Intel は米国 Intel Corporation の米国およびその他の国における商標または登録商標であり、使用許諾に基づいて使用しています。Microsoft および Windows は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに関する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。

初版：2012 年 8 月

製品番号：702113-291

目次

1 セキュリティの概要

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）ソフトウェアには、コンピューター、ネットワーク、および重要なデータに対する不正アクセスの防止に役立つセキュリティ機能があります。

アプリケーション	機能
HP ProtectTools Security Manager 管理者コンソール（管理者用）	• アクセスするには、Microsoft® Windows®の管理者権限が必要です • 管理者が設定したモジュールにアクセスできます。ユーザーはこれらのモジュールにはアクセスできません • セキュリティの初期セットアップを行えます。また、すべてのユーザーに適用されるオプションまたは要件を設定できます
HP ProtectTools Security Manager ユーザー コンソール（ユーザー用）	• ユーザーは管理者によって提供されたオプションを設定できます • 管理者は、一部の HP ProtectTools モジュールに対する限定的なコントロールをユーザーに提供できます

コンピューターで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、http://www.hp.com/jp/ を参照してください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools の機能

以下の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主要な機能
HP ProtectTools Security Manager 管理者コンソール	管理者は、以下の機能を実行できます ● HP ProtectTools Security Manager セットアップ ウィザードを使用して、セキュリティ レベルおよびセキュリティ ログイン方法を設定します ● ユーザーからは非表示になっているオプションを設定します ● Drive Encryption を有効にし、ユーザー アクセスを設定します ● Device Access Manager ポリシーおよびユーザー アクセスを設定します ● 管理者ツールを使用して、HP ProtectTools ユーザーを追加および削除したり、ユーザーの状態を表示したりします
HP ProtectTools Security Manager ユーザー コンソール	一般ユーザーは、以下の機能を実行できます ● 暗号化の状態の設定および Device Access Manager の設定を表示します ● Computrace for HP ProtectTools を有効にします ● [オプション]および[バックアップおよび復元]オプションを設定します
Credential Manager（資格情報マネージャー）	一般ユーザーは、以下の機能を実行できます ● ユーザー名およびパスワードを変更します ● Windows パスワード、指紋、顔の画像、スマート カード、近接型カード、非接触型カードなどユーザーの資格情報を設定および変更します
Password Manager（パスワード マネージャー）	一般ユーザーは、以下の機能を実行できます ● ユーザー名とパスワードを整理およびセットアップします ● 強固なパスワードを作成してアカウントのセキュリティを強化します。Password Manager は、この情報を自動的に入力して送信します ● ユーザーの資格情報を自動的に記憶して適用するシングルサインオン機能を使用してログオン プロセスを効率化します
Drive Encryption for HP ProtectTools（一部のモデルのみ）	● ハードドライブをボリューム全体にわたって完全に暗号化します ● データの暗号化解除やデータへのアクセスにブート前認証を強制します ● 自己暗号化ドライブを有効にするオプションを表示します（一部のモデルのみ）

モジュール	主要な機能
Device Access Manager for HP ProtectTools（一部のモデルのみ）	● IT 管理者が、ユーザー プロファイルに基づいてデバイスへのアクセスを制御できます ● 不正なユーザーが外部のストレージ メディアを使用してデータを削除したり、外部のメディアからシステムにウィルスを侵入させたりできないようにします ● 管理者が、特定の個人またはユーザーのグループに対して、通信デバイスへのアクセスを無効にできます
盗難からの回復（Computrace for HP ProtectTools、別売）	● 有効にするには、追跡契約およびトレース契約を別途購入する必要があります ● フォルダーやファイルを安全に管理できます ● ユーザー操作や、ソフトウェアとハードウェアの変更を監視します ● ハードドライブが再フォーマットまたは交換されてもアクティブな状態を維持します

HP ProtectTools セキュリティ製品の説明と一般的な使用例

HP ProtectTools セキュリティ製品のほとんどは、パスワードを紛失したり、利用できなくなったり、忘れたりした場合、または企業のセキュリティ部門で必要となった場合にコンピューターにアクセスするためのユーザー認証機能（通常はパスワード）および管理バックアップ機能を搭載しています。

注記： 一部の HP ProtectTools セキュリティ製品は、データへのアクセスを制限するように設計されています。データの重要性が非常に高いためデータを紛失するより危険にさらすことの方が懸念される場合には、データを暗号化する必要があります。すべてのデータは安全な場所にバックアップしておくことをおすすめします。

Password Manager（パスワード マネージャー）

Password Manager は、ユーザー名およびパスワードを格納します。次の用途に使用できます。

- インターネット アクセスまたは電子メールのログイン名およびパスワードを保存する
- ユーザーを Web サイトまたは電子メールに自動的にログインさせる
- 認証を管理および整理する
- Web またはネットワーク資産を選択して、リンクに直接アクセスする
- 必要に応じて名前およびパスワードを表示する

例 1：ある大規模メーカーの購買担当者は、その企業の取引のほとんどをインターネットで行っています。また、ログイン情報が必要となるいくつかの人気 Web サイトにもよくアクセスします。この購買担当者は、セキュリティに十分注意しているため、アカウントごとに異なるパスワードを使用しています。購買部では、Password Manager を使用して、Web リンクごとに異なるユーザー名およびパスワードを設定することにしました。購買担当者が Web サイトのログオン画面にアクセスすると、Password Manager によって資格情報が自動的に提供されます。ユーザー名およびパスワードが表示されるようにしたい場合は、Password Manager で設定できます。

Password Manager は、認証を管理および編集するためにも使用できます。ユーザーは、このツールを使用して、Web またはネットワーク資産を選択し、リンクに直接アクセスできます。また、必要に応じてユーザー名およびパスワードを表示することもできます。

例 2：ある多忙な公認会計士が、経理部全体を監督する立場に昇進しました。経理部では、多数のクライアントの Web アカウントに、それぞれ異なるログイン情報を使用してログオンする必要があります。このログイン情報は複数の社員で共有する必要があるため、機密保持が問題となります。そこで、すべての Web リンク、企業ユーザー名、およびパスワードを Password Manager 内で整理することにしました。整理を完了させ、Password Manager を社員に配布すれば、使用する資格情報を知らせないで社員に Web アカウントを利用させることができます。

Drive Encryption for HP ProtectTools（一部のモデルのみ）

Drive Encryption は、コンピューターのハードドライブ全体またはセカンダリ ドライブ上にあるデータへのアクセスを制限するために使用できます。また、Drive Encryption は自己暗号化ドライブも管理できます。

例 1：ある医師が、自分のコンピューターのハードドライブにあるどのデータにも自分しかアクセスできないようにしたいと考えています。そこで、この医師は Drive Encryption を有効にし、Windows のログイン前にブート前認証が求められるようにしました。セットアップを完了すれば、オペレーティング システムの起動前にパスワードを入力しなければハードドライブにアクセスできなくなります。自己暗号化ドライブ オプションでデータを暗号化するように選択すれば、ドライブのセキュリティをさらに強化することもできます。

Drive Encryption for HP ProtectTools は、暗号化したデータとハードドライブの両方をコンピューターのシステム ボードに関連付けるため、たとえハードドライブを取り外してもそのデータにはアクセスできません。

例 2：ある病院の経営者は、医師および承認されている人だけが、個人パスワードを共有することなく、自分たちのコンピューター内のデータにアクセスできるようにしたいと考えています。そこで、病院の IT 部門は、その経営者、医師、および承認されたすべての人を Drive Encryption ユーザーとして追加することにしました。これで、承認された人だけが個人のユーザー名およびパスワードを使用してコンピューターまたはドメインにログオンできるようになります。

Device Access Manager for HP ProtectTools（一部のモデルのみ）

Device Access Manager for HP ProtectTools を使用すると、管理者は、ハードウェアへのアクセスを制限および管理できます。Device Access Manager for HP ProtectTools は、データのコピーが可能な USB フラッシュ ドライブへの不正なアクセスをブロックするために使用できます。また、CD/DVD ドライブへのアクセス、USB デバイスの制御、ネットワーク接続などを制限することもできます。例えば、外部の業者が社内のコンピューターにアクセスできるようにすると同時に、その業者がデータを USB ドライブにコピーできないようにする必要がある場合が考えられます。

例 1：医薬品会社のあるマネージャーは、個人の医療記録と会社のデータを仕事でよく使用しています。他の社員もこのデータにアクセスする必要がありますが、そのデータが USB デバイスや他の外部ストレージ メディアによってコンピューターからコピーされないようにすることが大変重要です。ネットワークは安全ですが、コンピューターに CD ライターや USB ポートが搭載されているため、データがコピーされたり盗まれたりする可能性があります。そこで、このマネージャーは、Device Access Manager で CD ライターと USB ポートを無効にし、使用できないようにしました。たとえ USB ポートをブロックしても、マウスおよびキーボードは引き続き動作します。

例 2：ある保険会社では、社員が自宅にある個人のソフトウェアをインストールしたり、個人のデータを読み込んだりできないようにしたいと考えています。ただし、一部の社員は、すべてのコンピューターで USB ポートにアクセスする必要があります。そこで、この会社の IT 管理者は、Device

Access Manager を使用して、一部の社員に対してアクセスを許可すると同時に、その他の社員に対しては外部アクセスをブロックしました。

Computrace for HP ProtectTools（以前の LoJack Pro）（別売）

Computrace for HP ProtectTools（別売）は、盗難されたコンピューターがインターネットに接続されればいつでもその所在地を追跡できるサービスです。Computrace for HP ProtectTools を使用すると、コンピューターをリモートで管理および特定したり、コンピューターの使用状況やアプリケーションを監視したりできます。

例 1：ある学校の校長は、IT 部門に対し、学校にあるすべてのコンピューターを常時監視するように指示しました。そこで、学校の IT 管理者はコンピューターの保有状況を確認してから、すべてのコンピューターを Computrace に登録し、盗まれた場合に追跡できるようにしました。その後、この学校では、いくつかのコンピューターがなくなっていることに気づきました。そのため、IT 管理者は、警察に通報するとともに、Computrace の担当者に通知しました。これらのコンピューターは発見され、警察の手によって取り戻されて学校に返却されました。

例 2：ある不動産会社では、世界中にあるコンピューターの管理および更新が必要になりました。そこで、Computrace を使用して、IT 担当者を実際に現地に派遣しなくてもコンピューターの監視および更新が実行できるようにしました。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成

盗難からの保護

盗難の例として、空港の検問所での、機密データや顧客情報を含むコンピューターの盗難が挙げられます。盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。
  - Security Manager for HP ProtectTools：28 ページの「HP ProtectTools Security Manager」を参照してください。
  - Drive Encryption for HP ProtectTools：45 ページの「Drive Encryption for HP ProtectTools（一部のモデルのみ）」を参照してください。
- 暗号化は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。
- Computrace では、盗難の被害にあった後のコンピューターの場所を追跡できます。
  - Computrace for HP ProtectTools：67 ページの「盗難からの回復（一部のモデルのみ）」を参照してください。

機密データへのアクセス制限

契約検査官がオンサイトで作業していて、機密の財務データの確認のためにコンピューターへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、通信デバイスへのアクセスを制限できます。58 ページの「デバイス クラス構成」を参照してください。

内部または外部からの不正なアクセスの防止

セキュリティ保護されていないコンピューターへの不正なアクセスは、金融サービス、役員、または研究開発チームからのデータなどの社内ネットワーク リソースや、患者記録や個人の財務データなどの個人情報を非常に大きなリスクにさらすことになります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。
  - Security Manager for HP ProtectTools：28 ページの「HP ProtectTools Security Manager」を参照してください。
  - Drive Encryption for HP ProtectTools：45 ページの「Drive Encryption for HP ProtectTools（一部のモデルのみ）」を参照してください。
- Security Manager は、不正なユーザーがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。28 ページの「HP ProtectTools Security Manager」を参照してください。
- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、書き込み可能なデバイスへのアクセスを制限できます。55 ページの「Device Access Manager for HP ProtectTools（一部のモデルのみ）」を参照してください。

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）で、パスワードやシングルサインオンのための保護されたリポジトリが提供されます。28 ページの「HP ProtectTools Security Manager」を参照してください。

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピューターのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザーに割り当てることが重要な作業の 1 つです。

注記： 小さな組織や個人で使用する場合などは、一人の人がすべての役割を受け持つこともできます。

HP ProtectTools では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Drive Encryption などの配備するセキュリティ機能を決定します。

注記： HP ProtectTools の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、http://www.hp.com/jp/ を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者がスマート カードの配備を決定した場合、IT 管理者はパスワード モードおよびスマート カード モードの両方を有効にできます。
- ユーザー：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムでスマート カードを有効にしている場合、ユーザーはスマート カードの PIN を設定し、そのカードを認証に使用できます。

注意： 管理者は、エンド ユーザーの権限の制限や、ユーザー アクセスの制限に関して「ベスト プラクティス」に従うことをおすすめします。

権限のないユーザーには管理者権限を付与しないでください。

HP ProtectTools のパスワードの管理

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者のみが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザーまたは管理者が設定できます。

HP ProtectTools のパスワード	設定するモジュール	機能
Windows のログオン パスワード	Windows の[コントロール パネル]または HP ProtectTools Security Manager	HP ProtectTools Security Manager のさまざまな機能にアクセスするための手動ログオンまたは認証に使用できます
HP ProtectTools Security Manager の[バックアップおよび復元]パスワード	HP ProtectTools Security Manager（ユーザーごと）	HP ProtectTools Security Manager の[バックアップおよび復元]ファイルへのアクセスを保護します
スマート カードの PIN	Credential Manager（資格情報マネージャー）	マルチファクター認証として使用できます Windows 認証として使用できます スマート カードが選択されている場合は、Drive Encryption のユーザーを認証します

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを参考にしてください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させせます。
- 可能な場合は、常に半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの l または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分けます。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字を以下の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピューターのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピューター上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

資格情報および設定のバックアップ

以下の方法で資格情報をバックアップできます。

- Drive Encryption for HP ProtectTools を使用して、HP ProtectTools 資格情報の選択およびバックアップを行う
- インストール済みの HP ProtectTools モジュールからのセキュリティ証明書をバックアップし、復元するための中心となる場所として、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のバックアップおよび復元ツールを使用する

2 お使いになる前に

HP ProtectTools の設定を構成するには HP Client Security セットアップ ウィザードまたは HP ProtectTools Security Manager セットアップ ウィザードを使用します。

HP Client Security セットアップ ウィザードを完了すると、[HP Client Security]ダッシュボードにアプリケーションの状態が表示されます。

HP Client Security セットアップ ウィザード

注記： HP ProtectTools の管理には管理者権限が必要です。

HP Client Security セットアップ ウィザードでは、HP ProtectTools Security Manager で最もよく使用する機能を設定できます。まだ HP Client Security セットアップ ウィザードを完了していない場合は、以下のどちらかの方法で HP Client Security セットアップ ウィザードを起動できます。

▲ スタート画面で［**HP Client Security**］アプリケーションをクリックまたはタップします。

または

Windows デスクトップで［**HP ProtectTools**］ガジェットをクリックします。

ページは以下の順序で表示されます。

1. ［**Windows パスワード**］：Windows パスワードを入力します。

   強力な認証を使用して Windows アカウントを保護します。

2. ［**SpareKey**］：SpareKey オプションを登録するには、セキュリティに関する質問を 3 つ選択します。

3. ［**指紋の登録**］：指紋認証システムおよび対応ドライバーがインストールされている場合は、指紋を登録できます。少なくとも 2 つの指紋を選んで登録する必要があります。

4. ［**Drive Encryption**］：Drive Encryption for HP ProtectTools がインストールされている場合は、メイン ドライブの暗号化を有効にできます。

   - 従来のハードドライブの場合はソフトウェア暗号化
   - 自己暗号化ドライブが検出された場合はハードウェア暗号化

   暗号化を有効にする前に、以下のうち 1 つ以上の場所に暗号化キーを保存する必要があります。

注記： この時点でウィザードをキャンセルすると、Windows および Drive Encryption の認証を有効にできなくなります。

- **リムーバブル メディア**：FAT32 でフォーマットされた USB フラッシュ ドライブなどが使用できます。
  - [Drive Encryption]ページが表示される前に 1 つのリムーバブル デバイスが検出された場合は、初期設定でこのオプションが選択されます。
  - 2 つ以上のリムーバブル デバイスが検出された場合は、表示されたドライブのどれかを選択します。
- ［**SkyDrive**］：このオプションはインターネット接続が検出された場合にのみ選択できます。

  Windows Live ID が必要です。ID とパスワードを入力するか、ID を新規登録します。

5. 成功を示す通知が[完了]ページに表示され、Drive Encryption を有効にするために再起動するよう求められます。

HP ProtectTools Security Manager セットアップ ウィザード

注記： HP ProtectTools の管理には管理者権限が必要です。

HP ProtectTools Security Manager セットアップ ウィザードでは、HP ProtectTools Security Manager の機能を設定できます。ウィザードにある設定に加え、管理者であれば管理者コンソールを通じてその他の多くのセキュリティ機能を設定できます。これらの設定は、コンピューターおよびそのコンピューターを共有しているすべてのユーザーに適用されます。

HP ProtectTools Security Manager セットアップ ウィザードを起動するには、以下の操作を行います。

▲ 管理者コンソールの左側の枠内にある[**セットアップ ウィザード**]をクリックし、画面の説明に沿って操作してセットアップを完了させます。

管理者は HP ProtectTools Security Manager ユーザー コンソールから管理者コンソールを起動できます。詳しくは、16 ページの「HP ProtectTools Security Manager 管理者コンソール」を参照してください。

HP ProtectTools Security Manager およびそのアプリケーションは、このコンピューターを共有しているすべてのユーザーが使用できます。

[HP Client Security]ダッシュボード

既に HP Client Security セットアップ ウィザードを完了している場合に[HP Client Security]を開くには、以下の操作を行います。

▲ スタート画面で「hp」と入力して[**HP Client Security**]を選択します。

各アプリケーションの機能と関連する状態の概要がダッシュボードに表示されます。

▲ 特定のアプリケーションの詳細を表示するには、そのアプリケーションの行をクリックまたはタップします。

- [**今すぐ設定**]ボタンが表示されている場合は、アプリケーションがまだ設定されていないことを示します。このボタンをクリックまたはタップすると、アプリケーションを設定するためのページが開きます。
- [**設定**]ボタンが表示されている場合は、アプリケーションのステータスが OK であることを示します。このボタンをクリックまたはタップすると、アプリケーションの設定にアクセスできます。
- **ユーザーコンソール**は、ユーザー設定を行う場合に起動します。
- **管理者コンソール**は、管理者権限が必要な設定を行う場合に起動します。
- **[状態]ダッシュボード**はユーザー コンソールまたは管理者コンソールを起動しても開いたままであり、設定を構成してコンソールを閉じると状態が更新されます。

3 HP ProtectTools for Small Business イージー セットアップ ガイド

この章は、HP ProtectTools for Small Business 内の最も一般的で、かつ最も役立つオプションを有効にするための基本的な手順を示すように設計されています。このソフトウェアには、設定を微調整したり、アクセス制御を設定したりするために使用できる多数のツールやオプションが含まれています。このイージー セットアップ ガイドは、各モジュールを最小限の設定作業および時間で動作させることに重点を置いています。詳細情報を表示するには、対象のモジュールを選択し、右上隅にある[**?**]ボタンまたは[ヘルプ]ボタンをクリックします。このボタンによって、現在表示されているウィンドウでの作業に役立つ情報が自動的に表示されます。

お使いになる前に

1. Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックして HP ProtectTools Security Manager を開きます。
2. Windows パスワードを入力するか、作成します。
3. セットアップ ウィザードを完了します。

注記： 初期設定では、HP ProtectTools Security Manager は強力な認証ポリシーに設定されています。

この設定は、Windows にログインしている間の不正なアクセスを防止するために設計されており、高いセキュリティ レベルが必要な場合や、ユーザーが 1 日を通して頻繁にシステムから離れている場合に使用されます。この設定を変更する場合は、[セッション ポリシー]タブをクリックし、選択を行います。

Windows ログイン中に HP ProtectTools Security Manager によって 1 回のみ認証されるようにするには、以下の操作を行います。

1. Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックして HP ProtectTools Security Manager を開きます。
2. 左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。
3. 左側の枠内で、[**システム**]の[**セキュリティ**]グループから[**認証**]を選択します。
4. [**セッション ポリシー**]タブをクリックし、セッションの要件にするログイン情報の組み合わせを選択します。この選択を元に戻すには、[**初期設定に復元**]をクリックします。
5. 完了したら、[**適用**]ボタンをクリックします。

Password Manager（パスワード マネージャー）

パスワードはさまざまな場面で必要です。どのユーザーも多数のパスワードを使用します。定期的に Web サイトにアクセスしたり、ログオンの必要なアプリケーションを使用している場合は特にそうです。一般的なユーザーは、すべてのアプリケーションおよび Web サイトに同じパスワードを使用したり、パスワードの作成に凝っても、どのパスワードがどのアプリケーションのものかすぐに忘れてしまったりします。

Password Manager を使用すると、パスワードを自動的に記憶させるか、またはパスワードを記憶するサイトと省略するサイトをユーザーが識別できるようになります。コンピューターにサイン オンした後は、登録されているアプリケーションまたは Web サイトのパスワードまたは資格情報が Password Manager によって提供されます。

資格情報が必要な任意のアプリケーションまたは Web サイトにアクセスすると、Password Manager がそのサイトを自動的に認識し、ユーザーの情報をソフトウェアで記憶するかどうかをユーザーに尋ねます。特定のサイトを除外したい場合は、ユーザーの情報を記憶するという要求を辞退できます。

Web の場所、ユーザー名、およびパスワードの保存を開始するには、以下の操作を行います。

1. 登録されている Web サイトやアプリケーションなどにアクセスして、Web ページの左上隅にある[Password Manager]アイコンをクリックし、Web 認証を追加します。
2. リンクに名前を付け（オプション）、Password Manager にユーザー名およびパスワードを入力します。

注記： 現在および以降のアクセス時に Password Manager で使用する領域が強調表示されます。

3. 完了したら、[**OK**]ボタンをクリックします。
4. Password Manager には、ネットワーク共有またはネットワーク ドライブの割り当てのためのユーザー名およびパスワードを保存することもできます。

Password Manager（パスワード マネージャー）に保存されている認証の表示および管理

Password Manager を使用すると、中心となる場所から認証を表示、管理、バックアップ、および起動できます。また、Password Manager では、保存されているサイトの Windows からの起動もサポートされます。

Password Manager を開くには、以下のどちらかの操作を行います。

- ctrl ＋ Windows ロゴ キー＋ h ホット キーを使用して Password Manager を開きます。[**開く**]をクリックすると、保存されているショートカットがすばやく起動され、認証されます。

  または

- Password Manager で[**管理**]タブを選択して HP ProtectTools Security Manager を開きます。そこで、資格情報を編集できます。

Password Manager の[**編集**]オプションを使用すると、名前とログイン名を表示および変更できるほか、パスワードを表示することもできます。

HP ProtectTools for Small Business では、すべての資格情報および設定を別のコンピューターにバックアップしたり、コピーしたりできます。

Device Access Manager for HP ProtectTools

Device Access Manager を使用すると、データがハードドライブ上に安全な状態で残り、会社の外部に持ち出されることがないように、さまざまな内蔵および外付けストレージ デバイスの使用を制限できます。たとえば、あるユーザーにデータへのアクセスは許可するものの、CD、個人用音楽プレーヤー、または USB メモリ デバイスへのコピーをブロックするとします。これを設定するための簡単な方法を以下に示します。

1. Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックして HP ProtectTools Security Manager ユーザー コンソールを開きます。
2. HP ProtectTools Security Manager の左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。
3. [**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
4. 次の手順は、他のすべてのユーザーがブロックされた状態でも引き続きアクセスを可能にするユーザーの選択です。
5. 制限するハードウェア デバイスを選択し、[**適用**]ボタンをクリックして処理を完了します。
6. [**追加**]を選択し、[**詳細**]→[**今すぐ検索**]の順にクリックします。
7. 目的のユーザーを選択してから、[**OK**]→[**OK**]→[**適用**]の順にクリックします。

   選択内容が[**ユーザー/グループ**]ボックスに表示されます。
8. ユーザーが使用することになる[**デバイス クラス**]を選択し、[**許可**]または[**拒否**]を選択してから、[**適用**]をクリックします。

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools を使用すると、ハードドライブ全体を暗号化することによってデータを保護できます。コンピューターが盗まれたり、ハードドライブが元のコンピューターから取り外されて異なるコンピューターに接続されたりしたとしても、ハードドライブのデータは保護されたままになります。

また、Drive Encryption を使用すると、オペレーティング システムを起動する前にユーザー名とパスワードを使用して適切な認証をすることが必要になるため、セキュリティが強化されます。このプロセスはブート前認証と呼ばれます。

作業が簡単に実行できるように、Windows ユーザー アカウント、ドメイン、Drive Encryption for HP ProtectTools、Password Manager（パスワード マネージャー）、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）などさまざまなソフトウェア モジュールでパスワードが自動的に同期されます。

Drive Encryption for HP ProtectTools を有効にするには、以下の操作を行います。

1. Windows デスクトップで、タスクバーの右端の通知領域にある［**HP ProtectTools**］アイコンをダブルクリックして HP ProtectTools Security Manager を開きます。
2. 左側の枠内で、［**管理**］→［**管理者コンソール**］の順にクリックします。
3. 左側の枠内で［**セットアップ ウィザード**］をクリックします。
4. [ようこそ]画面で[**次へ**]を選択します。
5. Windows パスワードを入力して有効化ウィザードを起動してから、［**次へ**］をクリックします。
6. HP SpareKey を使用する必要がない場合は、HP SpareKey の登録作業をスキップします。
7. ［**Drive Encryption**］チェック ボックスにチェックを入れて、［**次へ**］をクリックします。
8. 暗号化するドライブにチェックを入れて、［**次へ**］をクリックします。
9. Drive Encryption の設定ウィンドウが表示され、暗号化リカバリ キーを保存するための USB フラッシュドライブまたはその他の外付けデバイスが要求されます。起動前パスワードを紛失した場合またはパスワードが機能しない場合に、このリカバリ キーをデータの復元やドライブへのアクセスに使用するため、リカバリ キーは安全な場所に確実に保管してください。
10. ［**次へ**］をクリックし、処理を完了してから、［**完了**］をクリックします。USB フラッシュ ドライブを取り外し、準備ができたらコンピューターを再起動します。
11. コンピューターが起動したら、Drive Encryption から Windows パスワードが要求されます。パスワードを入力し、［**OK**］をクリックします。

注記： ドライブの暗号化処理中は、コンピューターの動作が遅くなったように見える場合があります。完全に暗号化されると、パフォーマンスは正常に戻ります。このドライブ上のデータにアクセスすると、管理者が指定した要件に応じてデータが暗号化されたり暗号化が解除されたりします。

Drive Encryption 認証は Windows ログインに「チェーン」され、直接 Windows デスクトップが表示されるため、パスワードを 2 回入力する必要がなくなります。

4 HP ProtectTools Security Manager 管理者コンソール

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）ソフトウェアには、コンピューター、ネットワーク、および重要なデータに対する不正アクセスの防止に役立つセキュリティ機能があります。HP ProtectTools Security Manager の管理は、管理者コンソールの機能を通して提供されます。

また、HP ProtectTools Security Manager ユーザー コンソールでは、コンピューターを紛失した場合や盗難された場合に、見つけ出すための補助をする、追加のアプリケーションを利用できます（一部のモデルのみ）。

管理者コンソールを使用すると、ローカルの管理者は以下のタスクを実行できます。

- セキュリティ機能の有効化または無効化
- 認証に必要な資格情報の指定
- コンピューターのユーザーの管理
- デバイス固有のパラメーターの調整
- インストールされている HP ProtectTools Security Manager アプリケーションの設定

お使いになる前に

HP ProtectTools の設定を構成するには HP Client Security セットアップ ウィザードまたは HP ProtectTools Security Manager セットアップ ウィザードを使用します。

HP Client Security セットアップ ウィザードを完了すると、[HP Client Security]ダッシュボードにアプリケーションの状態が表示されます。

HP Client Security セットアップ ウィザード

注記： HP ProtectTools の管理には管理者権限が必要です。

HP Client Security セットアップ ウィザードでは、HP ProtectTools Security Manager で最もよく使用する機能を設定できます。まだ HP Client Security セットアップ ウィザードを完了していない場合は、以下のどちらかの方法で HP Client Security セットアップ ウィザードを起動できます。

▲ スタート画面で[**HP Client Security**]アプリケーションをクリックまたはタップします。

または

Windows デスクトップで[**HP ProtectTools**]ガジェットをクリックします。

ページは以下の順序で表示されます。

1. [**Windows パスワード**]：Windows パスワードを入力します。

   強力な認証を使用して Windows アカウントを保護します。

2. [**SpareKey**]：SpareKey オプションを登録するには、セキュリティに関する質問を 3 つ選択します。

3. [**指紋の登録**]：指紋認証システムおよび対応ドライバーがインストールされている場合は、指紋を登録できます。少なくとも 2 つの指紋を選んで登録する必要があります。

4. [**Drive Encryption**]：Drive Encryption for HP ProtectTools がインストールされている場合は、メイン ドライブの暗号化を有効にできます。

   - 従来のハードドライブの場合はソフトウェア暗号化
   - 自己暗号化ドライブが検出された場合はハードウェア暗号化

   暗号化を有効にする前に、以下のうち 1 つ以上の場所に暗号化キーを保存する必要があります。

   注記： この時点でウィザードをキャンセルすると、Windows および Drive Encryption の認証を有効にできなくなります。

   - **リムーバブル メディア**：FAT32 でフォーマットされた USB フラッシュ ドライブなどが使用できます。
     - [Drive Encryption]ページが表示される前に 1 つのリムーバブル デバイスが検出された場合は、初期設定でこのオプションが選択されます。
     - 2 つ以上のリムーバブル デバイスが検出された場合は、表示されたドライブのどれかを選択します。
   - [**SkyDrive**]：このオプションはインターネット接続が検出された場合にのみ選択できます。

     Windows Live ID が必要です。ID とパスワードを入力するか、ID を新規登録します。

5. 成功を示す通知が[完了]ページに表示され、Drive Encryption を有効にするために再起動するよう求められます。

HP ProtectTools Security Manager セットアップ ウィザード

注記： HP ProtectTools の管理には管理者権限が必要です。

HP ProtectTools Security Manager セットアップ ウィザードでは、HP ProtectTools Security Manager の機能を設定できます。ウィザードにある設定に加え、管理者であれば管理者コンソールを通じてその他の多くのセキュリティ機能を設定できます。これらの設定は、コンピューターおよびそのコンピューターを共有しているすべてのユーザーに適用されます。

HP ProtectTools Security Manager セットアップ ウィザードを起動するには、以下の操作を行います。

▲ 管理者コンソールの左側の枠内にある[**セットアップ ウィザード**]をクリックし、画面の説明に沿って操作してセットアップを完了させます。

管理者は HP ProtectTools Security Manager ユーザー コンソールから管理者コンソールを起動できます。詳しくは、16 ページの「HP ProtectTools Security Manager 管理者コンソール」を参照してください。

HP ProtectTools Security Manager およびそのアプリケーションは、このコンピューターを共有しているすべてのユーザーが使用できます。

[HP Client Security]ダッシュボード

既に HP Client Security セットアップ ウィザードを完了している場合に[HP Client Security]を開くには、以下の操作を行います。

▲ スタート画面で「`hp`」と入力して[**HP Client Security**]を選択します。

各アプリケーションの機能と関連する状態の概要がダッシュボードに表示されます。

▲ 特定のアプリケーションの詳細を表示するには、そのアプリケーションの行をクリックまたはタップします。

- [**今すぐ設定**]ボタンが表示されている場合は、アプリケーションがまだ設定されていないことを示します。このボタンをクリックまたはタップすると、アプリケーションを設定するためのページが開きます。
- [**設定**]ボタンが表示されている場合は、アプリケーションのステータスが OK であることを示します。このボタンをクリックまたはタップすると、アプリケーションの設定にアクセスできます。
- **ユーザーコンソール**は、ユーザー設定を行う場合に起動します。
- **管理者コンソール**は、管理者権限が必要な設定を行う場合に起動します。
- **[状態]ダッシュボード**はユーザー コンソールまたは管理者コンソールを起動しても開いたままであり、設定を構成してコンソールを閉じると状態が更新されます。

HP ProtectTools 管理者コンソールを開く

システム ポリシーの設定やソフトウェアの構成などの管理者タスクには、HP ProtectTools 管理者コンソールを使用します。管理者コンソールは、HP ProtectTools Security Manager を開くとアクセスできます。

1. Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックします。

   または

   [**コントロール パネル**]→[**システムとセキュリティ**]→[**HP ProtectTools Security Manager**]の順に選択します。

2. HP ProtectTools Security Manager ユーザー コンソールの左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。

管理者コンソールの使用

HP ProtectTools 管理者コンソールは、HP ProtectTools Security Manager の機能およびアプリケーションを管理するための中心となる場所です。

1. Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックします。

   または

   [**コントロール パネル**]→[**システムとセキュリティ**]→[**HP ProtectTools Security Manager**]の順に選択します。

2. HP ProtectTools Security Manager ユーザー コンソールの左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。

管理者コンソールの左側の枠内にある[ホーム]に、以下のセクションが表示されます。

- [**システム**]：ユーザーやデバイスの以下のセキュリティ機能および認証を設定できます。
  - [**セキュリティ**]
  - [**ユーザー**]
  - [**資格情報**]
- [**アプリケーション**]：HP ProtectTools Security Manager および HP ProtectTools Security Manager アプリケーションの設定を構成できます。
- [**データ**]：Drive Encryption（一部のモデルのみ）の設定を構成できます。
- [**コンピューター**]：Device Access Manager の設定を構成できます。
- [**セットアップ ウィザード**]：HP ProtectTools Security Manager を設定できます。
- [**バージョン情報**]：バージョン番号や著作権情報などの、HP ProtectTools Security Manager に関する情報を表示します。
- [**メイン領域**]：アプリケーション固有の画面を表示します。

[**?**]：管理者コンソールのヘルプが表示されます。このアイコンはウィンドウ枠の右上の最小化アイコンおよび最大化アイコンの隣にあります。

システムの設定

[**システム**]グループには、HP ProtectTools 管理者コンソールの画面の左側にあるメニュー パネルからアクセスします。このグループ内のアプリケーションを使用して、コンピューター、ユーザー、およびデバイスのポリシーや設定を管理できます。

[**システム**]グループには、以下のアプリケーションが含まれています。

- [**セキュリティ**]：このコンピューターに対する、ユーザーの対話操作の方法を管理する機能、認証、および設定を管理します。
- [**ユーザー**]：このコンピューターのユーザーを設定、管理、および登録します。
- [**資格情報**]：コンピューターに内蔵または接続されているセキュリティ デバイスの設定を管理したり、設定を構成したりします。

コンピューターでの認証の設定

認証アプリケーション内で、コンピューターへのアクセスを管理するポリシーを設定できます。Windows にログオンするとき、またはユーザー セッション中に Web サイトやプログラムにログオンするときに各クラスのユーザーを認証するために必要な資格情報を指定できます。

コンピューターでの認証を設定するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]→[**認証**]の順にクリックします。
2. ログオン認証を設定するには、[**ログオン ポリシー**]タブをクリックし、変更を行ってから[**適用**]をクリックします。
3. セッション認証を設定するには、[**セッション ポリシー**]タブをクリックし、変更を行ってから[**適用**]をクリックします。

ログオン ポリシー

Windows にログオンするときにユーザーを認証するために必要な資格情報を管理するポリシーを定義するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]→[**認証**]の順にクリックします。
2. [**ログオン ポリシー**]タブで、管理者や標準ユーザーなどのユーザー カテゴリを選択します。
3. 認証資格情報をクリックして編集ダイアログを表示します。
4. 2 つの認証資格情報を組み合わせる必要がある場合は、下向き矢印をクリックして各資格情報を選択し、[**OK**]をクリックします。
5. 資格情報を削除するには、[**X**]をクリックするか、資格情報を右クリックして[**削除**]をクリックします。
6. 確認ダイアログで[**はい**]をクリックします。
7. ユーザーがログオンできるかどうかを確認するには、[**Check that HP ProtectTools can log on**]（HP ProtectTools がログオンできることを確認）をクリックします。

8. 元の設定に戻すには、[**初期設定に復元**]をクリックします。
9. [**適用**]をクリックします。

セッション ポリシー

Windows セッション中に認証を行うために必要な資格情報を管理するポリシーを定義するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]→[**認証**]の順にクリックします。
2. [**セッション ポリシー**]タブで、管理者や標準ユーザーなどのユーザー カテゴリを選択します。
3. 認証資格情報をクリックして編集ダイアログを表示します。
4. 2 つの認証資格情報を組み合わせる必要がある場合は、下向き矢印をクリックして各資格情報を選択し、[**OK**]をクリックします。
5. 資格情報を削除するには、[**X**]をクリックするか、資格情報を右クリックして[**削除**]をクリックします。
6. 確認ダイアログで[**はい**]をクリックします。
7. ユーザーがログオンできるかどうかを確認するには、[**Check that HP ProtectTools can log on**]（HP ProtectTools がログオンできることを確認）をクリックします。
8. 元の設定に戻すには、[**初期設定に復元**]をクリックします。
9. [**適用**]をクリックします。

設定

BIOS レベルまたは Drive Encryption レベルで認証がすでに実行されている場合に、このコンピューターのユーザーが Windows のログオンを省略できるようにするには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]→[**設定**]の順にクリックします。
2. [**ワン ステップ ログオンを許可する**]：ワン ステップ ログオンを有効にするにはチェック ボックスにチェックを入れ、無効にするにはチェック ボックスのチェックを外します。
3. [**適用**]をクリックします。

ユーザーの管理

ユーザー アプリケーション内で、このコンピューターの HP ProtectTools ユーザーを監視したり管理したりできます。

すべての HP ProtectTools ユーザーが一覧表示され、HP ProtectTools Security Manager を使用して設定されたポリシーに対して検証されます。一覧表示および検証は、これらのユーザーが各ポリシーを満たすことができる適切な資格情報を登録しているかどうかに関係なく行われます。

ユーザーを管理するには、以下の設定のどれかを選択します。

- ユーザーを追加するには、[**追加**]をクリックします。
- ユーザーを削除するには、そのユーザーをクリックしてから[**削除**]をクリックします。

- ユーザーの追加の資格情報を設定するには、そのユーザーをクリックしてから[**登録**]をクリックします。
- 特定のユーザーのポリシーを確認するには、そのユーザーを選択してからウィンドウ下部のポリシーを確認します。

資格情報

資格情報アプリケーション内で、HP ProtectTools Security Manager によって認識される内蔵デバイスまたは接続されているセキュリティ デバイスで使用できる設定を構成できます。

HP SpareKey

Windows ログオンでの HP SpareKey 認証を許可するかどうかを設定し、SpareKey 登録時にユーザーに表示されるセキュリティに関する質問を管理できます。

1. HP SpareKey の登録中にユーザーに表示されるセキュリティに関する質問を選択します。

   最大 3 つの質問をユーザー自身で作成して指定したり、ユーザーが独自のパスフレーズを入力できるようにしたりできます。

2. Windows ログオンで[HP SpareKey]による復元を許可するには、チェック ボックスにチェックを入れます。
3. [**適用**]をクリックします。

指紋

コンピューターに指紋認証システムがインストールまたは接続されている場合、[指紋]ページに以下のタブが表示されます。

- [**登録**]：ユーザーが登録できる指紋の最小数と最大数を選択できます。

  また、指紋認証システムからすべてのデータをクリアすることもできます。

  > ⚠ **注意：** 指紋認証システムのすべてのデータをクリアすると、管理者を含む、すべてのユーザーの指紋データが消去されます。ログオン ポリシーで指紋のみを求めるようにしている場合は、すべてのユーザーがコンピューターにログオンできなくなることがあります。

- [**感度**]–：指を滑らせたときに指紋認証システムで使用される感度を調整するには、スライダーを移動します。

  指紋が常に認識されない場合は、より低い感度を選択することが必要な場合があります。この設定を高くすると指紋の読み取りの変化に対する感度が向上するため、誤って受け入れられる可能性が減ります。[**中-高**]に設定すると、セキュリティおよび利便性の適切な組み合わせが得られます。

- [**詳細設定**]：以下のオプションのどれかを選択して、節電し、視覚的情報を向上するように指紋認証システムを設定します。
  - [**Optimized**]（最適化）：指紋認証システムは、必要に応じて有効になります。指紋認証システムが最初に使用されるときに、わずかな遅延が発生する場合があります。
  - [**節電**]：指紋認証システムは応答が遅くなりますが、必要な電力は少なくなります。
  - [**通常の電力**]：指紋認証システムは常に使用できる状態ですが、この設定は電力を最も多く使用します。

顔

コンピューターに Web カメラが内蔵または接続されていて、Face Recognition プログラムがインストールされている場合、管理者はコンピューターの使い勝手とセキュリティが侵害される危険性の低さとの間でバランスを取るように Face Recognition のセキュリティ レベルを設定できます。

1. [**資格情報**]→[**顔**]の順にクリックします。
2. 利便性を高めるには、スライダーをクリックして左にスライドさせ、精度を高めるには、スライダーをクリックして右にスライドさせます。
   - [**利便性**]：登録したユーザーが、条件がよくない場合でも簡単にアクセスできるようにするには、スライダーのバーをクリックしてスライダーを[**利便性**]の位置まで動かします。
   - [**バランス**]：セキュリティと使い勝手を適度に両立させる場合、機密情報がある場合、または不正なログインを試みられる可能性がある場所にコンピューターがある場合には、スライダーのバーをクリックしてスライダーを[**バランス**]の位置まで動かします。
   - [**精度**]：登録したシーンまたは現在の照明の状態が通常よりも悪いときに、ユーザーをアクセスしづらくして、ユーザーが誤って受け入れられてしまう可能性を低くする場合には、スライダーのバーをクリックしてスライダーを[**精度**]の位置に移動します。
3. 設定を元の値に戻すには、[**初期設定に復元**]をクリックします。
4. [**適用**]をクリックします。

スマート カード

認証にスマート カードを使用するには、管理者が事前にスマート カードを初期化する必要があります。CSP および PKCS11 対応の標準的なスマート カードのほとんどが Windows でサポートされています。

スマート カードの初期化

HP ProtectTools Security Manager では、多くの種類のスマート カードがサポートされます。PIN 番号として使用できる文字の数と種類はそれぞれ異なる場合があります。通常は、HP ProtectTools でセキュリティ アルゴリズムに使用されるセキュリティ証明書および管理 PIN をインストールするためのツールがスマート カードの製造元から提供されます。

注記： スマート カード用のミドルウェアをインストールする必要があります。

1. 使用しているスマート カード用のミドルウェア（ActivIdentity スマート カード用の ActivClient 6.x など）を入手してインストールします。
2. スマート カードをリーダーに挿入します。

3. スマート カードを初期化（フォーマット）します。
   a. スマート カード初期化ツールを起動します。スマートカードをリーダーに挿入すると自動的に表示される場合もあります。
   b. 画面の説明に沿って操作し、PIN を設定します。
   c. 後で参照できるようにロック解除コードを書き留めます。
4. キー ペアおよび資格情報を作成します。
   a. HP ProtectTools 管理者コンソールを起動します。
   b. [**資格情報**]→[**スマート カード**]→[**管理**]タブの順にクリックします。
   c. [**スマート カードの初期化**]が選択されていることを確認します。
   d. PIN を入力し、[**適用**]をクリックしてから、画面の説明に沿って操作します。

      スマート カードが正しく初期化されたら、スマート カードを登録する必要があります。

スマート カードの登録

スマート カードを初期化したら、HP ProtectTools 管理者コンソールでそのスマート カードを認証方法として登録する必要があります。

1. [**セットアップ ウィザード**]をクリックします。
2. [**ようこそ**]画面で[**次へ**]をクリックします。
3. Windows パスワードを入力して、[**次へ**]をクリックします。
4. [**SpareKey**]ページで、[**HP SpareKey のセットアップのスキップ**]をクリックしてから（SpareKey 情報を更新しない場合）、[**次へ**]をクリックします。
5. [**セキュリティ機能を有効にする**]ページで、[**次へ**]をクリックします。
6. [**資格情報の選択**]ページで、[**スマート カード**]が選択されていることを確認して、[**次へ**]をクリックします。
7. [**スマート カード**]ページで、PIN を入力して、[**次へ**]をクリックします。
8. [**完了**]をクリックします。

スマート カードは HP ProtectTools Security Manager ユーザー コンソールで登録することもできます。詳しくは、[スマート カード]ページの右上にある青色の[**?**]アイコンをクリックして、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

スマート カードの設定

コンピューターにスマート カード リーダーがインストールまたは接続されている場合、[スマート カード]ページに 2 つのタブが表示されます。

- ［**設定**］：スマート カードが取り外されたときに自動的にロックするようにコンピューターを設定するには、[**スマート カードが取り出されたらコンピューターをロックする**]チェック ボックスにチェックを入れて、[**適用**]をクリックします。

  注記： コンピューターがロックされるのは、そのスマート カードが Windows へのログオン時の認証資格情報として使用されていた場合のみです。Windows へのログオンに使用されていなかったスマート カードを取り外しても、コンピューターはロックされません。

- ［**管理**］：以下のオプションから選択します。
  - ［**スマート カードの初期化**］：HP ProtectTools で使用するためにスマート カードを準備します。HP ProtectTools 以外で初期化され、非対称のキーペアと関連する証明書を含んでいるスマート カードを使用する場合は、特定の証明書による初期化が必要でない限り、再度初期化する必要はありません。
  - ［**Change smart card PIN**］（スマート カード PIN の変更）：スマート カードで使用する PIN を変更できます。
  - ［**HP ProtectTools データのみを消去**］：カードの初期化中に作成される HP ProtectTools 証明書のみを消去します。その他のデータはカードから消去されません。
  - ［**Erase all data on the smart card**］（スマート カードのすべてのデータの消去）：指定されたスマート カードのすべてのデータを消去します。カードは、HP ProtectTools またはその他のアプリケーションで使用できなくなります。

注記： スマート カードおよびそのカードに対応するミドルウェアでサポートされていない機能は使用できません。

▲ [**適用**]をクリックします。

非接触型カード

非接触型カードは、コンピューター チップが内蔵された小さいプラスチック製のカードです。コンピューター本体に非接触型カード リーダーが接続され、製造元から提供された対応ドライバーがインストール済みで、認証資格情報として非接触型カードが選択されている場合は、非接触型カードを認証に使用できます。HP ProtectTools では、以下の種類の非接触型カードをサポートしています。

- 非接触型 HID iCLASS メモリ カード
- 非接触型 MiFare Classic 1k、4k、および小型メモリ カード

▲ 非接触型カードを設定するには、リーダーのすぐ近くにカードを置き、画面の説明に沿って操作してから[**適用**]をクリックします。

近接型カード

近接型カードは、コンピューター チップが内蔵された小さいプラスチック製のカードです。コンピューター本体に近接型カード リーダーが接続され、製造元から提供された対応ドライバーがインストール済みで、認証資格情報として近接型カードが選択されている場合は、セキュリティ強化のために他の資格情報と組み合わせてこの近接型カードを使用できます。

▲ 近接型カードを設定するには、リーダーのすぐ近くにカードを置いて、[**適用**]クリックします。

Bluetooth

コンピューターに Bluetooth®機能が搭載済みで、認証資格情報として Bluetooth が選択され、Bluetooth 対応電話がコンピューターとペアリングされている場合は、セキュリティ強化のために他の資格情報と組み合わせて Bluetooth 対応電話を使用できます。Bluetooth の設定を指定するには、以下の操作を行います。

▲ サイレント認証を許可するには、チェック ボックスにチェックを入れて、[**適用**]をクリックします。

PIN

認証資格情報として PIN が選択されている場合は、セキュリティ強化のために他の資格情報と組み合わせて PIN を使用できます。PIN の設定を指定するには、以下の操作を行います。

1. 上向きまたは下向き矢印をクリックして、PIN の最小長を選択します。

   許可されている最小桁数は 8 桁です。

2. [**適用**]をクリックします。

アプリケーション

管理者コンソールの左側の枠内にある[アプリケーション]の[設定]ページには、現在インストールされている HP ProtectTools Security Manager アプリケーションの動作をカスタマイズできる 2 つのタブがあります。

▲ 管理者コンソールの左側の枠内の[**アプリケーション**]で、[**設定**]をクリックします。

[全般]タブ

[**全般**]タブでは、以下の設定を使用できます。

- [**管理者用のセットアップ ウィザードを自動的に起動しない**]：ログオン時にウィザードが自動的に開かないようにするには、このオプションを選択します。
- [**ユーザー用の使用開始準備ウィザードを自動的に起動しない**]：ログオン時にユーザーの設定が自動的に開かないようにするには、このオプションを選択します。

1. 特定の設定を有効にするには隣にあるチェック ボックスにチェックを入れ、設定を無効にするにはチェック ボックスのチェックを外します。
2. [**適用**]をクリックします。

[アプリケーション]タブ

管理者は、以下のアプリケーションを有効または無効にできます。

- ［**Status**］（状態）：すべてのアプリケーションに対する状態の表示を有効にするにはチェックボックスにチェックを入れ、無効にするにはチェック ボックスのチェックを外します。
- ［**Password Manager**］：コンピューターのすべてのユーザーに対して Password Manager を有効にします。

1. 特定の設定を有効にするには隣にあるチェック ボックスにチェックを入れ、設定を無効にするにはチェック ボックスのチェックを外します。
2. ［**適用**］をクリックします。

すべてのアプリケーションを工場出荷時の設定に戻すには、［**初期設定に復元**］ボタンをクリックします。

データ

管理者コンソールの左側の枠内にある[データ]セクションでは、以下のアプリケーションの設定を構成できます。

- ［**Drive Encryption**］：設定を構成したり、ドライブの状態を表示したりします。詳しくは、[Drive Encryption]ページの右上にある青色の［**?**］アイコンをクリックして、Drive Encryption ソフトウェアのヘルプを参照してください。

コンピューター

管理者コンソールの左側の枠内にある[コンピューター]セクションでは、以下の Device Access Manager アプリケーションの設定を構成できます。

- 簡易構成
- デバイス クラス構成
- ジャスト イン タイム認証（JITA）の構成
- 詳細設定

詳しくは、[Device Access Manager]ページの右上にある青色の［**?**］アイコンをクリックして、Device Access Manager ソフトウェアのヘルプを参照してください。

5　HP ProtectTools Security Manager

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用すると、お使いのコンピューターのセキュリティを大幅に強化できます。

プリロードされている HP ProtectTools Security Manager の各アプリケーション、および Web からいつでもダウンロードできる追加アプリケーションを使用して、以下のタスクを実行できます。

- ログオンおよびパスワードを管理する
- Windows オペレーティング システムのパスワードを簡単に変更する
- プログラムのオプションを設定する
- 指紋を利用してセキュリティと利便性を強化する
- 認証用のシーンを 1 つ以上登録する
- 認証用のスマート カードをセットアップする
- プログラムのバックアップおよび復元を実行する
- アプリケーションをさらに追加する

Security Manager（セキュリティ マネージャー）を開く

以下のどちらかの方法で HP ProtectTools Security Manager を開きます。

▲ Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックします。

または

[**コントロール パネル**]→[**システムとセキュリティ**]→[**HP ProtectTools Security Manager**]の順に選択します。

HP ProtectTools Security Manager ユーザー コンソールの使用

HP ProtectTools Security Manager ユーザー コンソールは、HP ProtectTools Security Manager の機能、アプリケーション、および設定に簡単にアクセスするための中心となる場所です。ユーザー コンソールには以下のコンポーネントが表示されます。

- **[ID カード]**：ログオン中のユーザー アカウントを識別する、Windows ユーザー名およびアイコンを表示します。
- **[セキュリティ アプリケーション]**：以下のカテゴリのセキュリティを設定できる、リンクの展開メニューを提供します。
  - **[ホーム]**：パスワードを管理したり、認証資格情報をセットアップしたり、セキュリティ アプリケーションの状態を確認したりします。
  - **[盗難からの回復]**：Computrace for HP ProtectTools（別売）
- **[マイ ログオン]**：Password Manager および Credential Manager によって認証資格情報を管理します。
- **[マイ データ]**：Drive Encryption によってデータのセキュリティを管理します。

注記： アプリケーションがインストールされていない場合、この項目は表示されません。

- **[マイ コンピューター]**：Device Access Manager によってコンピューターのセキュリティを管理します。

注記： アプリケーションがインストールされていない場合、この項目は表示されません。

- **[管理]**：管理者であれば、ここから管理者コンソールにアクセスして、セキュリティおよびユーザーを管理できます。
- **[詳細設定]**：以下のような追加機能にアクセスするためのコマンドが表示されます。
  - **[オプション]**：HP ProtectTools Security Manager の個人設定を実行できます。
  - **[バックアップおよび復元]**：データをバックアップまたは復元できます。
  - **[バージョン情報]**：バージョン番号や著作権情報などの、HP ProtectTools Security Manager に関する情報を表示します。
- **[メイン領域]**：アプリケーション固有の画面を表示します。
- **[?]**：HP ProtectTools Security Manager ユーザー コンソールのヘルプを表示します。このアイコンはウィンドウ枠の右上の最小化アイコンおよび最大化アイコンの隣にあります。

個人用 ID カード

ID カードは、ユーザーの名前およびユーザーが選択した写真を表示して、Windows アカウントの所有者を一意に識別します。ID カードは、Security Manager の各ページの左上隅に、目立つような形で表示されます。

名前の表示方法は変更できます。初期設定では、Windows のセットアップ中に選択した完全な Windows ユーザー名および画像が表示されます。

表示名を変更するには、以下の操作を行います。

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ユーザー コンソールの左上隅にある ID カードをクリックします。
3. このアカウントの Windows ユーザー名を表示するボックスをクリックし、新しい名前を入力して、[**保存**]ボタンをクリックします。

マイ ログオン

このグループに含まれるアプリケーションによって、ユーザーのデジタル ID をさまざまな面から管理できます。

- ［**Password Manager**］：クイック リンクを作成および管理します。クイック リンクを使用すると、Windows パスワード、指紋、顔、スマート カード、近接型カード、非接触型カード、Bluetooth 対応電話、または PIN による認証を行うことで、Web サイトおよびプログラムを起動し、ログオンできるようになります。
- ［**Credential Manager**］：Windows パスワードの変更、指紋の登録、または顔の登録を簡単に実行したり、スマート カード、非接触型カード、近接型カード、Bluetooth 対応電話、または PIN のセットアップを簡単に実行したりできるようにします。

管理者は、ダッシュボードの左下隅にある[**管理**]→[**Central Management**]（集中管理）の順にクリックして、使用可能な追加のセキュリティ アプリケーションに関する情報にアクセスできます。

Password Manager（パスワード マネージャー）

Password Manager を使用すると、Windows、Web サイト、およびアプリケーションへのログオンがより簡単かつ安全になります。Password Manager によって、書き留めたり覚えたりする必要がなく強固なパスワードを作成しておき、実際のログオンは、指紋、顔、スマート カード、近接型カード、非接触型カード、PIN、または Windows パスワードを使用してすばやく簡単に行えます。

Password Manager には以下のオプションがあります。

[管理]タブ

- ログオンを追加、編集、または削除する。
- クイック リンクを使用して初期設定のブラウザーを起動し、セットアップ済みの Web サイトまたはプログラムにログオンする。
- ドラッグ アンド ドロップ操作でクイック リンクをカテゴリ別に整理する。
- セキュリティ上のリスクがあるパスワードがあるかどうかを確認する。

[パスワード強度]タブ

- Web サイトおよびアプリケーションに使用されている各パスワードの強度および全体的なパスワード強度を確認する。
- パスワード強度は、赤色、黄色、または緑色の状態インジケーターで表される。

［**Password Manager**］アイコンは、Web ページまたはアプリケーションのログオン画面の左上隅に表示されます。Web サイトまたはアプリケーション用のログオン情報が作成されていない場合は、プラス記号（＋）がアイコン上に表示されます。

▲ ［**Password Manager**］アイコンをクリックしてコンテキスト メニューを表示すると、以下のオプションを選択できます。

- [任意のドメイン]を Password Manager に追加
- Password Manager を開く
- アイコンの設定
- ヘルプ

ログオン情報が作成されていない Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- ［**[任意のドメイン]を Password Manager に追加**］：表示中のログオン画面用にログオンを追加できます。
- ［**Password Manager を開く**］：Password Manager を起動します。
- ［**アイコンの設定**］：［**Password Manager**］アイコンを表示する条件を指定できます。
- ［**ヘルプ**］：HP ProtectTools Security Manager のヘルプを表示します。

ログオン情報が作成されている Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- ［**ログオン データの入力**］：[ID の検証]ページを表示します。正しく認証されると、ログオン データがログオン用フィールドに自動的に入力され、ページが送信されます（ログオンを作成または最後に編集したときに送信を指定していた場合）。
- ［**ログオンの編集**］：表示中の Web サイト用のログオン データを編集できます。
- ［**ログオンの追加**］：アカウントを Password Manager に追加できます。
- ［**Password Manager を開く**］：Password Manager を起動します。
- ［**ヘルプ**］：HP ProtectTools Security Manager のヘルプを表示します。

注記： HP ProtectTools Security Manager は、資格情報を確認するときに、複数の資格情報が求められるようにコンピューターの管理者によってセットアップされていることがあります。

ログオン情報の追加

Web サイトまたはプログラム用のログオンは、ログオン情報を 1 回入力すれば、簡単に追加できます。以降は、Password Manager（パスワード マネージャー）によって情報が自動的に入力されるようになります。これらのログオンは、その Web サイトまたはプログラムを表示すると使用できるようになります。また、Password Manager の［**クイック リンク**］メニューからログオンをクリックし、Password Manager でその Web サイトまたはプログラムを表示させてログオンすることもできます。

ログオン情報を追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [**Password Manager**]アイコンの矢印をクリックし、ログオン画面の種類（Web サイト用またはプログラム用）に応じて以下のどちらかをクリックします。
   - Web サイトの場合は、[**[任意のドメイン]を Password Manager に追加**]をクリックします。
   - プログラムの場合は、[**Password Manager へのログオンの追加**]をクリックします。
3. ログオン データを入力します。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。[**Password Manager Manage**]（パスワード マネージャーの管理）タブから[**ログオンの追加**]をクリックするか、ctrl ＋ Windows ロゴ キー＋ h ホットキーを使用するか、または指を滑らせてこのダイアログ ボックスを表示させることもできます。

   a. あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。

   b. このログオン用のパスワードを表示するには、[**パスワードを表示する**]をクリックします。

   c. ログオン用フィールドの入力後に送信を実行しない場合は、[**ログオン データを自動的に送信する**]チェック ボックスのチェックを外します。

   d. [**OK**]をクリックして使用する認証方法（指紋、顔、スマート カード、近接型カード、非接触型カード、Bluetooth 対応電話、PIN、またはパスワード）を選択し、選択した認証方法を使用してログオンします。

      [**Password Manager**]アイコンのプラス記号（＋）が消え、ログオン情報が作成されたことが示されます。

   e. Password Manager でログオン用フィールドが検出されない場合は、[**その他のフィールド**]をクリックします。

      - ログオンに必要な各フィールドのチェック ボックスにチェックを入れ、ログオンに不要なフィールドのチェック ボックスのチェックを外します。
      - [**閉じる**]をクリックします。

この Web サイトまたはプログラムにアクセスすると、そのたびに Web サイトまたはアプリケーションのログオン画面の左上隅に[**Password Manager**]アイコンが表示され、登録済みの資格情報を使用してログオンできることが示されます。

ログオンの編集

ログオンを編集するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. ログオン情報を編集できるダイアログ ボックスを表示するには、[**Password Manager**]アイコンの矢印→[**ログオンの編集**]の順にクリックします。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。

   [**Password Manager Manage**]（パスワード マネージャーの管理）タブから[**目的のログオンの編集**]をクリックして、このダイアログ ボックスを表示させることもできます。

3. ログオン情報を編集します。
   - [**ユーザー名**]ログオン フィールドであらかじめフォーマットが用意された選択肢の 1 つを選択するには、フィールドの右側にある矢印をクリックします。
   - [**パスワード**]ログオン フィールドであらかじめフォーマットが用意された選択肢の 1 つを選択するには、フィールドの右側にある矢印をクリックします。
   - 画面上の他のフィールドをログオンに追加するには、[**その他のフィールド**]をクリックします。
   - このログオン用のパスワードを表示するには、[**パスワードを表示する**]をクリックします。
   - ログオン用フィールドの入力後に送信を実行しない場合は、[**ログオン データを自動的に送信する**]チェック ボックスのチェックを外します。
4. [**OK**]をクリックします。

Password Manager の[クイック リンク]メニューの使用

Password Manager では、ログオンを作成した Web サイトおよびプログラムをすばやく簡単に起動できます。Password Manager の[**クイック リンク**]メニューまたは[**管理**]タブからプログラムまたは Web サイトのログオンをダブルクリックし、ログオン画面を表示して、ログオン データを入力します。

作成したログオンは、Password Manager の[**クイック リンク**]メニューに自動的に追加されます。

[**クイック リンク**]メニューを表示するには、以下の操作を行います。

1. [**Password Manager**]のホットキー（ctrl ＋ Windows ロゴ キー＋ h が工場出荷時の設定です）を押します。ホットキーを変更するには、HP ProtectTools Security Manager ユーザー コンソールで[**Password Manager**]をダブルクリックし、[**設定**]をクリックします。
2. （指紋認証システムが内蔵または接続されたコンピューターで）指紋をスキャンするか、Windows パスワードを入力します。

ログオンをカテゴリ別に整理

ログオンを整理するには、1 つ以上のカテゴリを作成します。その後、ログオンを目的のカテゴリにドラッグ アンド ドロップします。

カテゴリを追加するには、以下の操作を行います。

1. HP ProtectTools Security Manager ユーザー コンソールで[**Password Manager**]をクリックします。
2. [**管理**]タブ→[**カテゴリの追加**]の順にクリックします。
3. カテゴリの名前を入力します。
4. [**OK**]をクリックします。

ログオンをカテゴリに追加するには、以下の操作を行います。

1. マウス ポインターを目的のログオンの上に置きます。
2. マウスの左ボタンを押したままにします。

3. ログオンをカテゴリの一覧にドラッグします。マウス ポインターをカテゴリの上に置くと、そのカテゴリが強調表示されます。

4. 目的のカテゴリが強調表示されたら、マウス ボタンを放します。

ログオンは、選択したカテゴリに移動されるのではなく、コピーされるのみです。そのため、同じログオンを複数のカテゴリに追加できます。[**すべて**]をクリックするとすべてのログオンを表示できます。

ログオンの管理

Password Manager を使用すると、ユーザー名、パスワード、および複数のログオン アカウントのログオン情報を、中心となる 1 つの場所から簡単に管理できます。

ログオン情報は[**管理**]タブに一覧表示されます。同じ Web サイトに対して複数のログオンが作成されている場合、各ログオンはその Web サイト名の下に一覧表示され、ログオン一覧の中でインデント表示されます。

ログオンを管理するには、以下の操作を行います。

▲ HP ProtectTools Security Manager ユーザー コンソールで、[**Password Manager**]→[**管理**]タブの順にクリックします。

- [**ログオンの追加**]：[**ログオンの追加**]をクリックし、画面の説明に沿って操作します。
- [**ログオン**]：既存のログオンをクリックし、以下のオプションのどれかを選択し、画面の説明に沿って操作します。
  - [**開く**]：既存のログオンがある Web サイトまたはプログラムを開きます。
  - [**追加**]：ログオンを追加します。詳しくは、31 ページの「ログオン情報の追加」を参照してください。
  - [**編集**]：ログオンを編集します。詳しくは、32 ページの「ログオンの編集」を参照してください。
  - [**削除**]：既存のログオンがある Web サイトまたはプログラムを削除します。
- [**カテゴリの追加**]：[**カテゴリの追加**]をクリックし、画面の説明に沿って操作します。詳しくは、33 ページの「ログオンをカテゴリ別に整理」を参照してください。

Web サイトまたはプログラムに他のログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。

2. [**Password Manager**]アイコンをクリックして、コンテキスト メニューを表示します。

3. [**ログオンの追加**]をクリックし、画面の説明に沿って操作します。

パスワード強度の評価

資格情報を保護するには、Web サイトおよびプログラムに強固なパスワードを使用することが重要です。

Password Manager では、Web サイトおよびプログラムへのログオンに使用されている各パスワードの強度を自動的にすばやく分析することで、セキュリティを監視および強化できます。

[**パスワード強度**]タブに、Web サイトおよびアプリケーションに使用されている各パスワードの強度および全体的なパスワード強度が、赤色、黄色、または緑色の状態インジケーターで表されます。

Password Manager（パスワード マネージャー）アイコンの設定

Password Manager は、Web サイトおよびプログラムのログオン画面を識別します。ログオン情報が作成されていないログオン画面が検出されると、Password Manager によってプラス記号（＋）の付いた[**Password Manager**]アイコンが表示され、そのログオン画面用のログオンを追加するよう求められます。

1. ログオン可能なサイトでの Password Manager の動作方法をカスタマイズするには、アイコン→[**アイコンの設定**]の順にクリックします。
   - [**ログオン画面へのログオンの追加を要求**]：ログオンがまだ設定されていないログオン画面が表示されたときに、Password Manager によってログオンの追加が求められるようにするには、このオプションをクリックします。
   - [**この画面を除外する**]：Password Manager による、このログオン画面へのログオンの追加を求めるメッセージが以後表示されないようにするには、このチェック ボックスにチェックを入れます。

     以前に除外した画面用のログオンを追加するには、以下の操作を行います。

     ◦ 以前に除外した Web サイト ログオンまたはプログラム ページが表示されているときに、HP ProtectTools Security Manager ユーザー コンソールを開き、[**Password Manager**]をクリックします。

     ◦ [**ログオンの追加**]をクリックします。

       [ログオンの追加]ダイアログ ボックスが開き、[**Current screen**]（現在の画面）フィールドに Web サイトのログオン画面またはプログラムが表示されます。

     ◦ [**続行**]をクリックします。

       [[パスワード マネージャー]へのログオンの追加]画面が表示されます。

     ◦ 画面に表示される説明に沿って操作します。詳しくは、31 ページの「ログオン情報の追加」を参照してください。

     ◦ [**Password Manager**]アイコンは、Web サイト ログオンまたはプログラム画面が開かれるたびに表示されます。

     [**ログオン画面のログオンを追加するかどうか確認しない**]：ラジオ ボタンを選択します。
2. Password Manager の詳細設定にアクセスするには、HP ProtectTools Security Manager ユーザー コンソールで[**Password Manager**]をダブルクリックし、[**設定**]をクリックします。

設定

Password Manager では、以下の個人設定を指定できます。

1. [**ログオン画面へのログオンの追加を要求**]：Web サイトまたはプログラムのログオン画面が検出されるたびに[**Password Manager**]アイコンをプラス記号（＋）付きで表示し、この画面のログオンを[**ログオン**]メニューに追加できることを示します。この機能を無効にするには、[**ログオン画面へのログオンの追加を要求**]の横にあるチェック ボックスのチェックを外します。
2. [**Open Password Manager with ctrl+win+h**]（ctrl ＋ win ＋ h でパスワード マネージャーを開く）：Password Manager の[**クイック リンク**]メニューを開くための初期設定のホットキーは、ctrl ＋ Windows ロゴ キー＋ h です。このホットキーを変更するには、このオプションをクリックして新しいキーの組み合わせを入力します。ctrl、alt、shift、および任意の英数字キーを組み合わせることができます。
3. [**適用**]をクリックして変更を保存します。

Credential Manager

HP ProtectTools Security Manager の資格情報を使用してお使いの ID を検証します。このコンピューターの管理者は、Windows アカウント、Web サイト、またはプログラムにログオンするユーザーが ID の確認に使用できる資格情報の種類を設定できます。

使用できる資格情報は、このコンピューターに内蔵または接続されているセキュリティ デバイスの種類によって異なります。[**マイ ログオン**]の下の[**Credential Manager**]をクリックするとサポートされている資格情報、要件、および現在の状態が一覧表示されるほか、以下のどれかまたはすべての情報が含まれます。

- パスワード
- HP SpareKey
- 指紋
- 顔
- スマート カード
- 非接触型カード
- 近接型カード
- Bluetooth
- PIN

資格情報を登録または変更するには、その資格情報のリンクをクリックし、画面の説明に沿って操作します。

Windows パスワードの変更

HP ProtectTools Security Manager を使用すると、Windows の[コントロール パネル]を使用するよりも、すばやく簡単に Windows パスワードを変更できます。

Windows パスワードを変更するには、以下の操作を行います。

1. HP ProtectTools Security Manager ユーザー コンソールで、[**Credential Manager**]→[**パスワード**]の順にクリックします。
2. [**現在の Windows パスワード**]テキスト ボックスに、現在のパスワードを入力します。
3. [**新しい Windows パスワード**]テキスト ボックスに新しいパスワードを入力し、[**新しいパスワードの確認**]テキスト ボックスにそのパスワードを再度入力します。
4. [**変更**]をクリックすると、現在のパスワードが、入力した新しいパスワードにすぐに変更されます。

HP SpareKey のセットアップ

HP SpareKey を使用すると、管理者によって定義済みの一覧からセキュリティに関する 3 つの質問に回答して、（サポートされているプラットフォーム上の）コンピューターにアクセスできます。

HP ProtectTools Security Manager セットアップ ウィザードの初期セットアップ時に、個人用の HP SpareKey をセットアップするよう求めるメッセージが表示されます。

HP SpareKey をセットアップするには、以下の操作を行います。

1. ウィザードの[SpareKey]ページで、セキュリティに関する質問を 3 つ選択し、各質問の回答を入力します。
2. [**作成**]をクリックします。

[**Credential Manager**]の下の[SpareKey]ページで、別の質問を選択したり、回答を変更したりできます。

HP SpareKey がセットアップされた後、ブート前ログオン画面または Windows の[ようこそ]画面から HP SpareKey を使用してコンピューターにアクセスできます。

指紋の登録

[**資格情報の選択**]画面で管理者が[指紋]を選択し、コンピューター本体に指紋認証システムが搭載または接続されている場合は、HP ProtectTools Security Manager セットアップ ウィザードの説明に沿って指紋を設定（指紋認証システムの用語としては「登録」）します。HP ProtectTools Security Manager ユーザー コンソールの[**Credential Manager**]の下の[指紋]ページでも指紋を登録できます。

1. ウィザードの[指紋]ページに、両手の輪郭が表示されます。すでに登録されている指は強調表示されます。輪郭で示されている指をクリックします。

   注記： 以前に登録された指紋を削除するには、その指紋に対応する指をクリックします。

2. 登録する指を選択すると、指紋が正常に登録されるまでその指を滑らせるよう求められます。登録された指は、輪郭が付いて強調表示されます。
3. 少なくとも 2 本の指を登録する必要があります。人差し指または中指をおすすめします。別の指を登録するには、手順 1 および 2 を繰り返します。
4. [**次へ**]をクリックし、画面の説明に沿って操作します。

注意： ウィザードで指紋を登録している場合は、手順 4 の[**次へ**]をクリックするまでは指紋の情報が保存されません。コンピューターをしばらくアイドル状態にしていた場合や、プログラムを閉じた場合は、それ以前に行った変更が保存されません。

顔認証ログオンのシーンの登録

コンピューター本体に Web カメラが内蔵または接続されている場合に顔認証ログオンを選択すると、HP ProtectTools Security Manager セットアップ ウィザードで、シーンを登録するよう求めるメッセージが表示されます。HP ProtectTools Security Manager ユーザー コンソールの[**Credential Manager**]の下の[顔]のログオン ページでもシーンを登録できます。

顔認証ログオンを使用するには、1 つ以上のシーンを登録する必要があります。正しく登録した後でも、以下の条件の 1 つ以上が変わったためにログオンが難しくなった場合には、新しいシーンを登録できます。

- 前回登録したときから顔つきが大きく変わった。
- 以前に登録したときと周囲の明るさが大幅に異なる。
- 前回の登録時に眼鏡をかけていた（またはかけていなかった）。

注記： シーンをうまく登録できない場合は、Web カメラにもっと近づいてください。

HP ProtectTools Security Manager セットアップ ウィザードからシーンを登録するには、以下の操作を行います。

1. ウィザードの[顔]ログオン ページで、[**詳細設定**]をクリックし、追加のオプションを設定します。詳しくは、40 ページの「詳細ユーザー設定」を参照してください。
2. [**OK**]をクリックします。
3. [**開始**]をクリックするか、以前にシーンを登録したことがある場合は、[**新しいシーンの登録**]をクリックします。
4. シーンの登録中にデモ画面を見るには、[**動画の再生**]をクリックします。

   これが最初の登録である場合は、デモ画面を見るかどうかを確認するダイアログが表示されます。[**はい**]または[**いいえ**]をクリックします。
5. 照明が暗い場合は、ソフトウェアによって自動的に画面が明るくなります。また、背景の照明を変更するには、電球の形のアイコンをクリックします。
6. [**カメラ**]アイコンをクリックし、画面の説明に沿って操作して、シーンを登録します。

   注記： シーンを撮影している間、指示に従って顔の向きを決め、自分の画像を見るようにしてください。
7. [**次へ**]をクリックします。

HP ProtectTools Security Manager ユーザー コンソールからもシーンを登録できます。

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. [**マイ ログオン**]で、[**Credential Manager**]→[**顔**]の順にクリックします。
3. [**詳細設定**]をクリックし、追加のオプションを設定します。詳しくは、40 ページの「詳細ユーザー設定」を参照してください。

4. [**OK**]をクリックします。
5. [**開始**]をクリックするか、以前にシーンを登録したことがある場合は、[**新しいシーンの登録**]をクリックします。
6. Windows パスワードの入力を求めるメッセージが表示されたら、パスワードを入力して、[**次へ**]をクリックします。
7. シーンの登録中にデモ画面を見るには、[**動画の再生**]をクリックします。

   これが最初の登録である場合は、デモ画面を見るかどうかを確認するダイアログが表示されます。[**はい**]または[**いいえ**]をクリックします。
8. 照明が暗い場合は、ソフトウェアによって自動的に画面が明るくなります。また、背景の照明を変更するには、電球の形のアイコンをクリックします。
9. [**カメラ**]アイコンをクリックし、画面の説明に沿って操作して、シーンを登録します。

注記： シーンを撮影している間、指示に従って顔の向きを決め、自分の画像を見るようにしてください。

詳細については、[顔]の登録ページの右上にある青色の[**?**]アイコンをクリックして、Face Recognition ソフトウェアのヘルプを参照してください。

認証

1 つ以上のシーンを登録したら、認証に自分の顔を使用して、コンピューターにログオン、または新しい Windows セッションを開始できるようになります。

1. 認証画面が起動してカメラがユーザーの顔を検出すると、5 秒後にログオン プロセスが開始されます。顔が正しく認証されると、コンピューターにアクセスできます。
2. 顔認証ログオンがタイムアウトになると､Face Recognition は一時停止します。認証プロセスを再開するには、[**カメラ**]アイコンをクリックします。

注記： 照明が不足しており、Face Recognition を使用してログオンできない場合は、Windows パスワードを入力してコンピューターにログオンできます。

3. コンピューターにログオンしたときに、今後のログイン セッションでログオンが成功しやすくなるようにシーンの追加を求めるメッセージが Face Recognition で表示されたら、[**はい**]をクリックします。

暗所モード

照明が非常に暗い場所で顔認証ログオンを実行する場合は、顔認証ログオン画面の背景色が自動的に白に切り替わり、顔により明るい照明を当てたような状態になります。

顔認証ログオン画面の背景色を手動で切り替えるには、電球の形のアイコンをクリックします。

学習

顔認証ログオンには失敗してもパスワードの入力には成功した場合は、今後の顔認証ログオンが成功する確率を高めるためにさまざまな画像を保存するよう求められることがあります。

シーンの削除

現在登録されているシーンを削除するには、以下の操作を行います。

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. [**マイ ログオン**]で、[**Credential Manager**]→[**顔**]の順にクリックします。
3. 削除するシーン→[**ごみ箱**]アイコンの順にクリックします。
4. 確認ダイアログの[**OK**]をクリックします。

詳細ユーザー設定

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. [**マイ ログオン**]で、[**Credential Manager**]→[**顔**]の順にクリックします。
3. [**詳細設定**]をクリックし、以下のオプションを設定します。

   [**その他の設定**]タブ：以下のオプションを有効にするには、チェック ボックスにチェックを入れます（複数選択可）。オプションを無効にするには、チェック ボックスのチェックを外します。この設定は現在のユーザーにのみ適用されます。

   - [**顔認識のイベントでサウンドを再生する**]：顔認証ログオンが成功または失敗したときに音を鳴らします。
   - [**ログオンに失敗したら、シーンの更新を要求する**]：顔認証ログオンには失敗してもパスワードの入力には成功した場合に、今後の顔認証ログオンが成功する確率を高めるためにさまざまな画像を保存するよう求めるメッセージが表示されます。
   - [**ログオンに失敗したら、新しいシーンの登録を要求する**]：顔認証ログオンには失敗してもパスワードの入力には成功した場合に、今後の顔認証ログオンが成功する確率を高めるために新しいシーンを登録するよう求めるメッセージが表示されます。
4. 設定を元の値に戻すには、[**初期設定に復元**]をクリックします。
5. [**OK**]をクリックします。

スマート カードのセットアップ

コンピューター本体にスマート カード リーダーが内蔵または接続され、管理者が認証資格情報としてスマート カードを有効にして、HP ProtectTools 管理者コンソールのソフトウェア ヘルプで説明されている手順を実行した場合は、HP ProtectTools Security Manager セットアップ ウィザードでスマート カードを挿入して設定するよう求めるメッセージが表示されます。HP ProtectTools Security Manager ユーザー コンソールの[**Credential Manager**]の下の[スマート カード]ページでもスマート カードをセットアップできます。

注記： スマート カードを使用するには、管理者が事前にスマート カードを初期化する必要があります。

スマート カードの初期化

HP ProtectTools Security Manager では、多くの種類のスマート カードがサポートされます。PIN 番号として使用できる文字の数と種類はそれぞれ異なる場合があります。通常は、HP ProtectTools でセキュリティ アルゴリズムに使用されるセキュリティ証明書および PIN 管理をインストールするためのツールがスマート カードの製造元から提供されます。

管理者は、製造元が提供するソフトウェアおよび HP ProtectTools 管理者コンソールを使用してスマート カードを初期化できます。詳しくは、HP ProtectTools 管理者コンソール ソフトウェアのヘルプを参照してください。

スマート カードの登録

スマート カードを初期化した後、Security Manager で登録できます。

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. [**Credential Manager**]→[**スマート カード**]の順にクリックします。
3. [**セットアップ**]が選択されていることを確認します。
4. Windows パスワードおよび PIN を入力して、[**保存**]をクリックします。

管理者は、HP ProtectTools 管理者コンソールでスマート カードを登録することもできます。詳しくは、HP ProtectTools 管理者コンソール ソフトウェアのヘルプを参照してください。

スマート カードの PIN の変更

スマート カードの PIN を変更するには、以下の操作を行います。

1. すでにフォーマットされて初期化されているスマート カードを挿入します。
2. [**スマート カードの暗証番号の変更**]を選択します。
3. 古い PIN を入力してから、新しい PIN を入力および確認入力します。

非接触型カード

非接触型カードは、コンピューター チップが内蔵された小さいプラスチック製のカードです。コンピューター本体に非接触型カード リーダーが接続され、管理者が製造元から提供された対応ドライバーをインストールし、認証資格情報として非接触型カードを有効にしている場合は、認証資格情報として非接触型カードを使用できます。HP ProtectTools では、以下の種類の非接触型カードをサポートしています。

- 非接触型 HID iCLASS メモリ カード
- 非接触型 MiFare Classic 1k、4k、および小型メモリ カード

▲ 非接触型カードを設定するには、リーダーのすぐ近くにカードを置き、画面の説明に沿って操作してから[**適用**]をクリックします。

近接型カード

近接型カードは、コンピューター チップが内蔵された小さいプラスチック製のカードです。コンピューター本体に近接型カード リーダーが接続され、管理者が製造元から提供された対応ドライバーをインストールし、認証資格情報として近接型カードを有効にしている場合は、セキュリティ強化のために他の資格情報と組み合わせて近接型カードを使用できます。

▲ 近接型カードを設定するには、リーダーのすぐ近くにカードを置き、画面の説明に沿って操作してから[**適用**]をクリックします。

Bluetooth

管理者が認証資格情報として Bluetooth を有効にしている場合は、セキュリティ強化のために他の資格情報と組み合わせて Bluetooth 対応電話を設定できます。

注記： Bluetooth 対応の電話デバイスのみがサポートされています。

1. Bluetooth 機能がコンピューターで有効になっていること、および Bluetooth 対応電話が検出モードに設定されていることを確認します。電話を接続するには、自動生成されたコードを Bluetooth デバイスで入力することが必要になる場合があります。Bluetooth デバイスの構成設定によっては、コンピューターと電話のペアリング コードを比較することが必要になる場合があります。
2. 電話を登録するには、その電話を選択して、[**登録**]をクリックします。
3. 確認ダイアログで[**OK**]をクリックします。

PIN

管理者が認証資格情報として PIN を有効にしている場合は、セキュリティ強化のために他の資格情報と組み合わせて PIN を設定できます。

▲ 新しい PIN を設定するには、PIN を入力してから、その PIN を再び入力して確認します。

管理

管理者は、HP ProtectTools Security Manager ユーザー コンソールの左下パネルにある[**管理**]をクリックし、[**管理者コンソール**]を選択すると、[Central Management]（集中管理）にアクセスできます。

詳しくは、HP ProtectTools 管理者コンソール ソフトウェアのヘルプを参照してください。

詳細設定

ユーザー コンソールの左下パネルにある[**詳細設定**]をクリックして、以下のオプションにアクセスできます。

- [**設定**]：HP ProtectTools Security Manager の個人設定を実行できます。
- [**バックアップおよび復元**]：HP ProtectTools Security Manager データをバックアップまたは復元できます。
- [**バージョン情報**]：HP ProtectTools Security Manager のバージョン情報を表示します。

オプションの設定

HP ProtectTools Security Manager では、個人設定を指定できます。HP ProtectTools Security Manager ユーザー コンソールで、**[詳細設定]**→**[オプション]**の順にクリックします。使用可能な設定が、**[全般]**と**[指紋]**の 2 つのタブに表示されます。

[全般]タブ

[外観]：**[タスク バーの通知領域にアイコンを表示する]**

- タスク バーへのアイコンの表示を有効にするには、このチェック ボックスにチェックを入れます。
- タスク バーへのアイコンの表示を無効にするには、このチェック ボックスのチェックを外します。

[指紋]タブ

注記： **[指紋]**タブは、コンピューターに指紋認証システムおよび正しいドライバーがインストールされている場合にのみ表示されます。

- **[クイック アクション]**：クイック アクションを使用すると、割り当てたキーを押したまま、指を滑らせて指紋を読み取らせたときに実行される HP ProtectTools Security Manager のタスクを選択できます。

  クイック アクションを一覧のどれかのキーに割り当てるには、**[（キー）＋指紋]**オプションをクリックして、使用可能なタスクをメニューから 1 つ選択します。
- **[指紋スキャンのフィードバック]**：指紋認証システムが使用できる場合にのみ表示されます。この設定を使用すると、指紋を読み取らせたときに返されるフィードバックを調整できます。
  - **[サウンド フィードバックを有効にする]**：指紋が読み取られたときに、HP ProtectTools Security Manager によってサウンドのフィードバックが返されます。プログラム イベントごとに異なるサウンドが再生されます。Windows の[コントロール パネル]にある[サウンド]設定の**[サウンド]**タブでイベントに新しいサウンドを割り当てるか、このオプションを選択解除してサウンドのフィードバックを無効にできます。
  - **[スキャン品質フィードバックを表示する]**

    品質に関係なくすべてのスキャンを表示するには、このチェック ボックスにチェックを入れます。

    高品質のスキャンのみを表示するには、このチェック ボックスのチェックを外します。

データのバックアップおよび復元

Security Manager のデータは定期的にバックアップすることをおすすめします。バックアップの頻度は、データが変更される頻度によって決まります。たとえば、毎日のように新しいログオンを追加している場合は、データを毎日バックアップする必要があります。

また、他のコンピューターへの移行時にバックアップを使用することもできます。この作業は、インポートおよびエクスポートと呼ばれます。

注記： Password Manager および Face Recognition の情報のみがこの機能でバックアップされます。Drive Encryption には独自のバックアップ方法が用意されています。Device Access Manager および指紋認証の情報はバックアップされません。

バックアップ ファイルからデータを復元できるようにするには、バックアップ データを取り込むコンピューターに HP ProtectTools Security Manager をインストールしておく必要があります。

データをバックアップするには、以下の操作を行います。

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ユーザー コンソールの左の枠内で、[**詳細設定**]→[**バックアップおよび復元**]の順にクリックします。
3. [**データのバックアップ**]をクリックします。
4. バックアップに含めるモジュールを選択します。多くの場合、すべてのモジュールを選択します。
5. ID を検証します。
6. ストレージ ファイルの名前を入力します。初期設定では、このファイルはユーザーの[ドキュメント]フォルダーに保存されます。別の場所を指定するには、[**参照**]をクリックします。
7. ファイルを保護するためのパスワードを入力します。
8. [**完了**]をクリックします。

データを復元するには、以下の操作を行います。

1. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ユーザー コンソールの左の枠内で、[**詳細設定**]→[**バックアップおよび復元**]の順にクリックします。
3. [**データの復元**]をクリックします。
4. 以前に作成したストレージ ファイルを選択します。表示されているフィールドにパスを入力して、[**参照**]をクリックします。
5. ファイルを保護するために使用しているパスワードを入力します。
6. データを復元するモジュールを選択します。多くの場合、表示されるすべてのモジュールを選択します。
7. Windows パスワードを検証します。
8. [**完了**]をクリックします。

6 Drive Encryption for HP ProtectTools（一部のモデルのみ）

Drive Encryption for HP ProtectTools は、コンピューターのデータを暗号化することによって完全なデータ保護を可能にします。Drive Encryption を有効にしている場合は、Windows オペレーティング システムが起動する前に表示される、Drive Encryption のログイン画面からログオンする必要があります。

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の[HP Client Security]セットアップ ウィザード、[詳細設定]ウィザード、または管理者コンソールを使用すると、Windows 管理者は、Drive Encryption の有効化、暗号化キーのバックアップ、および暗号化するドライブやパーティションの選択または選択解除を行えます。詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

Drive Encryption では、以下のタスクを実行できます。

- Drive Encryption の設定の選択：
  - TPM（Trusted Platform Module）で保護されたパスワードの有効化
  - ソフトウェアによる暗号化を使用した個々のドライブまたはパーティションの暗号化または暗号化の解除
  - ハードウェアによる暗号化を使用した自己暗号化ドライブの暗号化または暗号化の解除
  - Drive Encryption のブート前認証が常に要求されるようにスリープまたはスタンバイ状態を無効にすることによる、一層のセキュリティ強化

注記： 暗号化できるドライブは内蔵 SATA ハードドライブおよび外付け eSATA ハードドライブのみです。

- バックアップ キーの作成
- バックアップ キーおよび HP SpareKey を使用した、暗号化されたコンピューターへのアクセスの復元
- パスワード、登録された指紋、または一部の対応するスマートカードの PIN を使用した Drive Encryption のブート前認証の有効化

Drive Encryption を開く

管理者は HP ProtectTools Security Manager ユーザー コンソールを開いて Drive Encryption にアクセスできます。

1. Windows デスクトップで、タスクバーの右端の通知領域にある［**HP ProtectTools**］アイコンをダブルクリックします。

   または

   ［**コントロール パネル**］→［**システムとセキュリティ**］→［**HP ProtectTools Security Manager**］の順に選択します。

2. HP ProtectTools Security Manager ユーザー コンソールの左側の枠内で、［**管理**］→［**管理者コンソール**］の順に選択します。

3. HP ProtectTools 管理者コンソールの左側の枠内で［**Drive Encryption**］を選択します。

一般的なタスク

標準ハードドライブに対する Drive Encryption の有効化

標準ハードドライブはソフトウェアによる暗号化を使用して暗号化されます。Drive Encryption を有効にするには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールを起動します。詳しくは、19 ページの「HP ProtectTools 管理者コンソールを開く」を参照してください。

2. 左側の枠内で［**セットアップ ウィザード**］をクリックします。

3. ［**Drive Encryption**］チェック ボックスにチェックを入れ、［**次へ**］をクリックします。

4. 暗号化キーをバックアップするには、 このキーを記録するための外付けデバイスを接続します。このキーは、ほかの方法で失敗した場合にデータにアクセスするために使用する必要があります。

5. ［**Drive Encryption キーのバックアップ**］で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。

6. ［**次へ**］をクリックします。

注記： コンピューターの再起動を求めるメッセージが表示されます。再起動すると、Drive Encryption のブート前認証画面が表示され、Windows が起動する前に認証を求めるメッセージが表示されます。

Drive Encryption が有効になりました。選択したドライブのパーティションの数やサイズによっては、パーティションの暗号化に数時間かかる場合があります。

詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

自己暗号化ドライブに対する Drive Encryption の有効化

自己暗号化ドライブの管理に関する Trusted Computing Group の OPAL 仕様に適合する自己暗号化ドライブは、ソフトウェアによる暗号化またはハードウェアによる暗号化を使用して暗号化できます。自己暗号化ドライブに対して Drive Encryption を有効にするには、以下の操作を行います。

注記： ハードウェアによる暗号化は、お使いのコンピューターのすべてのドライブが自己暗号化ドライブであり、自己暗号化ドライブの管理に関する Trusted Computing Group の OPAL 仕様に適合している場合にのみ使用できます。その場合は、[**ドライブのハードウェア暗号化を使用**]オプションが使用可能になるため、ハードウェアによる暗号化またはソフトウェアによる暗号化のどちらかを使用できます。

自己暗号化ドライブと標準ハードドライブが混在している場合は、[**ドライブのハードウェア暗号化を使用**]オプションが使用できなくなるため、ソフトウェアによる暗号化のみを使用できます。詳しくは、46 ページの「標準ハードドライブに対する Drive Encryption の有効化」を参照してください。

▲ Drive Encryption を有効にするには、HP ProtectTools Security Manager セットアップ ウィザードを使用します。

または

ソフトウェアによる暗号化

1. HP ProtectTools 管理者コンソールを起動します。詳しくは、19 ページの「HP ProtectTools 管理者コンソールを開く」を参照してください。
2. 左側の枠内で[**セットアップ ウィザード**]をクリックします。
3. [**Drive Encryption**]チェック ボックスにチェックを入れ、[**次へ**]をクリックします。

   注記： 画面下部の[**ドライブのハードウェア暗号化を使用**]オプションが使用可能になっている場合は、このチェック ボックスのチェックを外します。

4. [**暗号化するドライブ**]で、暗号化するハードドライブのチェック ボックスにチェックを入れ、[**次へ**]をクリックします。
5. 暗号化キーをバックアップするには、適切なスロットにストレージ デバイスを挿入します。
6. [**Drive Encryption キーのバックアップ**]で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。
7. [**適用**]をクリックします。

   注記： コンピューターが再起動されます。

   Drive Encryption が有効になりました。ドライブのサイズによっては、ドライブの暗号化に何時間もかかることがあります。

ハードウェアによる暗号化

1. HP ProtectTools 管理者コンソールを起動します。詳しくは、19 ページの「HP ProtectTools 管理者コンソールを開く」を参照してください。
2. 左側の枠内で[**セットアップ ウィザード**]をクリックします。
3. [**Drive Encryption**]チェック ボックスにチェックを入れ、[**次へ**]をクリックします。

4. 画面下部の[**ドライブのハードウェア暗号化を使用**]チェック ボックスを使用できる場合は、チェックが入っていることを確認します。

   このチェック ボックスにチェックが入っていないか、またはチェック ボックス自体を使用できない場合は、ソフトウェアによる暗号化が適用されます。詳しくは、46 ページの「標準ハードドライブに対する Drive Encryption の有効化」を参照してください。

5. [**暗号化するドライブ**]で暗号化するハードドライブのチェック ボックスにチェックを入れ、[**次へ**]をクリックします。

   注記： ドライブが 1 つだけ表示される場合は、そのドライブのチェック ボックスが自動的に選択され、グレーで表示されます。

   複数のドライブが表示される場合は、ディスク 0 も自動的に選択されてグレーで表示されますが、さらに別のハードドライブを選択するためのオプションを使用できるようになります。このオプションによって、ハードウェアによるドライブの暗号化を別のハードドライブでも有効にできます。

   [**次へ**]ボタンは 1 つ以上のドライブが選択されるまで使用できません。

6. 暗号化キーをバックアップするには、適切なスロットにストレージ デバイスを挿入します。

7. [**Drive Encryption キーのバックアップ**]で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。

8. [**適用**]をクリックします。

   注記： コンピューターの再起動を求めるメッセージが表示されます。Drive Encryption のブート前認証画面が表示され、Windows の起動前に認証を求めるメッセージが表示されます。

   Drive Encryption が有効になりました。ドライブの暗号化に数分かかることがあります。

詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

Drive Encryption の無効化

管理者は、HP ProtectTools Security Manager セットアップ ウィザードを使用して Drive Encryption を無効にできます。詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

1. HP ProtectTools 管理者コンソールを起動します。詳しくは、19 ページの「HP ProtectTools 管理者コンソールを開く」を参照してください。

2. 左側の枠内で[**セットアップ ウィザード**]をクリックします。

3. [**Drive Encryption**]チェック ボックスのチェックを外し、[**次へ**]をクリックします。

   Drive Encryption の無効化が開始されます。

注記： ソフトウェアによる暗号化が使用されていた場合は、暗号化の解除が開始されます。暗号化されていたハードドライブ パーティションのサイズによっては、暗号化の解除に数時間かかることがあります。暗号化の解除が完了すると、Drive Encryption が無効になります。

ハードウェアによる暗号化が使用されていた場合は、ドライブの暗号化がすぐに解除され、数分後に Drive Encryption が無効になります。

Drive Encryption が無効になると、ハードウェアによる暗号化が使用されていた場合はコンピューターのシャットダウンを求めるメッセージが表示されます。ソフトウェアによる暗号化が使用されていた場合は、コンピューターの再起動を求めるメッセージが表示されます。

Drive Encryption の有効化後のログイン

Drive Encryption が有効になり、ユーザー アカウントが登録された後でコンピューターを起動した場合、Drive Encryption のログイン画面からログオンする必要があります。

注記： スリープまたはスタンバイ状態から復帰するときは、ソフトウェアによる暗号化でもハードウェアによる暗号化でも、Drive Encryption のブート前認証画面は表示されません。ハードウェアによる暗号化では[**スリープ モードの無効化によるセキュリティの強化**]オプションが用意されていて、これを有効にするとスリープまたはスタンバイ状態が発生しないようにすることができます。

ハイバネーション状態から復帰するときは、ソフトウェアによる暗号化でもハードウェアによる暗号化でも、Drive Encryption のブート前認証画面が表示されます。

注記： Windows 管理者が HP ProtectTools Security Manager で BIOS ブート前セキュリティを有効にしていて、ワンステップ ログオンが有効になっている場合（初期設定では有効）は、BIOS ブート前セキュリティで認証を行った直後にコンピューターにログオンできます。Drive Encryption のログイン画面による再認証は求められません。

1 人のユーザーのログオン：

▲ [**ログオン**]ページで、Windows のパスワード、スマート カードの PIN、または HP SpareKey を入力するか、顔認証を使用するか、登録した指の指紋を認証システムで読み取らせます。

複数のユーザーのログオン：

1. [**ログオンするユーザーの選択**]ページで、ドロップダウン リストからログオンするユーザーを選択して、[**次へ**]をクリックします。
2. [**ログオン**]ページで、Windows のパスワードまたはスマート カードの PIN を入力するか、または登録した指の指紋を認証システムで読み取らせます。

注記： 以下のスマート カードがサポートされます。

サポートされているスマート カード

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

注記： Drive Encryption のログイン画面で復元キーを使用してログオンする場合、ユーザー アカウントにアクセスするには、Windows のログオン画面で追加の資格情報を入力するように求められます。

ハードドライブの暗号化によるデータの保護

HP ProtectTools Security Manager セットアップ ウィザードでハードドライブを暗号化してデータを保護することを強くおすすめします。暗号化を有効にすると、追加したハードドライブや作成したパーティションを以下の手順で暗号化できます。

1. 左側のパネルで、[**Drive Encryption**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
2. [**設定**]をクリックします。
3. ソフトウェアによって暗号化するドライブについては、暗号化するドライブ パーティションを選択します。

注記： これは、1 つ以上の標準ハードドライブと 1 つ以上の自己暗号化ドライブが存在する混合ドライブのシナリオにも該当します。

または

▲ ハードウェアによって暗号化するドライブについては、暗号化する追加のドライブを選択します。

高度なタスク

Drive Encryption の管理（管理者のタスク）

管理者は[Drive Encryption]の下の[設定]ページで、Drive Encryption の状態（有効、無効、またはハードウェアによる暗号化が有効）を表示および変更し、コンピューター上のすべてのハードドライブの暗号化の状態を表示できます。

注記： [Drive Encryption]の[設定]ページでは、追加したハードドライブのみを対象として、ハードウェアによる暗号化の選択または選択解除を行えます。

- 状態が無効の場合、Drive Encryption は Windows 管理者によって有効にされておらず、ハードドライブは保護されていません。Drive Encryption を有効にするには、HP ProtectTools Security Manager セットアップ ウィザードを使用します。
- 状態が有効の場合、Drive Encryption は有効にされ、設定されています。ドライブは、次のどれかの状態になっています。

ソフトウェアによる暗号化

- 暗号化されていない
- 暗号化されている
- 暗号化を実行中
- 暗号化解除を実行中

ハードウェアによる暗号化

- 暗号化されている
- 暗号化されていない（追加のドライブ）

TPM によって強化されたセキュリティの使用（一部のモデルのみ）

TPM（Trusted Platform Module）を有効にし、TPM による Drive Encryption セキュリティの強化機能を選択すると、Drive Encryption パスワードは TPM セキュリティ チップによって保護されます。ハードドライブが取り外されて別のコンピューターに取り付けられるようなことがあっても、そのハードドライブへのアクセスは拒否されます。

注意： TPM のオーナーシップを Windows TPM.msc と共有することはできません。

注記： パスワードは TPM セキュリティ チップで保護されているため、ハードドライブを別のコンピューターに移動すると、TPM 設定をそのコンピューターに移行しない限り、データにアクセスできなくなります。

注記： BIOS セットアップで[TPM]オプションを有効にしておく必要があります。

個々のドライブ パーティションの暗号化または暗号化の解除（ソフトウェアによる暗号化のみ）

管理者は[Drive Encryption]の[設定]ページを使用して、コンピューター上の 1 つまたは複数のハードドライブ パーティションを暗号化するか、またはすでに暗号化されているドライブ パーティションの暗号化を解除することができます。

1. HP ProtectTools 管理者コンソールを起動します。詳しくは、19 ページの「HP ProtectTools 管理者コンソールを開く」を参照してください。
2. 左側のパネルで、[**Drive Encryption**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**設定**]をクリックします。
4. [**ドライブの状態**]で、暗号化するか、または暗号化を解除する各ハードドライブの横にあるチェック ボックスにチェックを入れるか、またはチェックを外して、[**適用**]をクリックします。

注記： ドライブ パーティションの暗号化または暗号化解除が行われている間、暗号化されているパーティションの割合および処理が完了するまでの残り時間が進行状況バーに表示されます。

注記： ダイナミック パーティションはサポートされていません。パーティションが使用可能として表示されるが、選択しても暗号化できない場合、そのパーティションはダイナミック パーティションです。ダイナミック パーティションは、[ディスクの管理]で新しいパーティションを作成するためにどれかのパーティションを縮小した結果生成されます。

パーティションがダイナミック パーティションに変換される場合は、警告が表示されます。

バックアップおよび復元（管理者のタスク）

Drive Encryption が有効な場合、管理者は[暗号化キーのバックアップ]ページを使用して暗号化キーをリムーバブル メディアにバックアップしたり、復元を実行したりできます。

暗号化キーのバックアップ

管理者は、暗号化されたドライブの暗号化キーをリムーバブル ストレージ デバイスにバックアップできます。

注意： バックアップ キーを含むストレージ デバイスは必ず安全な場所に保管してください。パスワードを忘れた場合、スマート カードを紛失した場合、または、指紋を登録していない場合に、このデバイスがコンピューターにアクセスする唯一の方法となります。ストレージ デバイスを使用することで Windows にアクセスできるため、保管場所の安全も確保してください。

注記： 暗号化キーを保存するには、FAT32 または FAT16 でフォーマットされた USB ストレージ デバイスを使用する必要があります。バックアップには USB メモリ スティック、SD（Secure Digital）メモリ カード、またはマルチメディアカード（MMC）を使用できます。

1. HP ProtectTools 管理者コンソールを起動します。詳しくは、19 ページの「HP ProtectTools 管理者コンソールを開く」を参照してください。
2. 左側のパネルで、[**Drive Encryption**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**暗号化キーのバックアップ**]をクリックします。
4. 暗号化キーのバックアップに使用するストレージ デバイスを挿入します。

   注記： 暗号化キーを保存するには、FAT32 でフォーマットされた USB ストレージ デバイスを使用する必要があります。バックアップには USB メモリ スティック、SD（Secure Digital）メモリ カード、またはマルチメディアカード（MMC）を使用できます。SkyDrive を使用できる場合もあります。

5. [**ドライブ**]で、暗号化キーをバックアップするデバイスのチェック ボックスにチェックを入れます。
6. [**キーをバックアップする**]をクリックします。
7. 表示されるページに記載されている情報を読み、[**OK**]をクリックします。選択したストレージ デバイスに暗号化キーが保存されます。

暗号化が有効になっているコンピューターでのバックアップ キーを使用したアクセスの復元

管理者は、暗号化を有効にしたときにリムーバブル ストレージ デバイスにバックアップした Drive Encryption キー、または HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の[**Drive Encryption キーのバックアップ**]オプションを選択することでバックアップした Drive Encryption キーを使用して、復元を実行できます。

1. バックアップ キーが保管されているリムーバブル ストレージ デバイスを装着します。
2. コンピューターの電源を入れます。
3. Drive Encryption for HP ProtectTools のログイン ダイアログ ボックスが表示されたら、[**オプション**]をクリックします。
4. [**復元**]をクリックします。
5. バックアップ キーを含むファイル名またはパスを入力して、[**復元**]をクリックします。

   または

[**参照**]をクリックして必要なバックアップ ファイルを探し、[**OK**]をクリックしてから[**復元**]をクリックします。

6. 確認ダイアログ ボックスが表示されたら、[**OK**]をクリックします。

   Windows のログオン画面が表示されます。

   注記： Drive Encryption のログイン画面で復元キーを使用してログインする場合、ユーザー アカウントにアクセスするには、Windows のログオン画面で追加の資格情報を入力するように求められます。復元を実行した後は、パスワードを再設定することを強くおすすめします。

HP SpareKey のリカバリの実行

Drive Encryption のブート前認証で HP SpareKey のリカバリを実行する場合は、セキュリティに関する質問に正しく答えないとコンピューターにアクセスできません。HP SpareKey のリカバリの設定について詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

パスワードを忘れてしまった場合に HP SpareKey のリカバリを実行するには、以下の操作を行います。

1. コンピューターの電源を入れます。
2. [Drive Encryption for HP ProtectTools]ページが表示されたら、ユーザー ログオン ページに移動します。
3. [**SpareKey**]をクリックします。

   注記： HP ProtectTools Security Manager で HP SpareKey が初期化されていない場合は、[**SpareKey**]ボタンを使用できません。

4. 表示された質問に対して正しい回答を入力し、[**ログオン**]をクリックします。

   Windows のログオン画面が表示されます。

注記： Drive Encryption のログオン画面で HP SpareKey を使用してログオンする場合、ユーザー アカウントにアクセスするには、Windows のログオン画面で追加の資格情報を入力するように求められます。復元を実行した後は、パスワードを再設定することを強くおすすめします。

暗号化の状態の表示

ユーザーは HP ProtectTools Security Manager で暗号化の状態を表示できます。

注記： 管理者は HP ProtectTools 管理者コンソールを使用して Drive Encryption の状態を変更できます。

1. HP ProtectTools ユーザー コンソールを起動します。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ［マイ データ］で［**Drive Encryption**］をクリックします。

   ソフトウェアによる暗号化またはハードウェアによる暗号化のシナリオでは、ドライブ暗号化の状態が以下のどちらかとして表示されます。

   - 有効
   - 無効

   ソフトウェアによる暗号化のシナリオでは、ハードドライブまたはハードドライブ パーティションごとに、ドライブ暗号化の状態が以下のどれかとして表示されます。

   - 暗号化されていない
   - 暗号化されている
   - 暗号化を実行中
   - 暗号化解除を実行中

   ハードウェアによる暗号化のシナリオでは、ドライブ暗号化の状態が以下のどちらかとして表示されます。

   - 暗号化されていない
   - 暗号化されている

   ハードドライブの暗号化または暗号化解除を実行中、暗号化または暗号化解除が完了した割合および完了するまでの残り時間が進行状況バーに表示されます。

7 Device Access Manager for HP ProtectTools（一部のモデルのみ）

HP ProtectTools Device Access Manager は、データ転送デバイスを無効にすることによってデータへのアクセスを制御します。

注記： マウス、キーボード、タッチパッド、指紋認証システムなどの一部のヒューマン インターフェイス デバイスや入力デバイスは、Device Access Manager によって制御されません。詳しくは、65 ページの「管理されないデバイス クラス」を参照してください。

HP ProtectTools Device Access Manager を使用すると、Windows オペレーティング システムの管理者は、システム上のデバイスへのアクセスを制御し、不正なアクセスを防止できます。

- アクセスを許可または拒否するデバイスを定義するためのデバイス プロファイルが、ユーザーごとに作成されます。
- ジャスト イン タイム認証（JITA）を使用すると、あらかじめ定義されたユーザーは、通常はアクセスできないデバイスにアクセスするために、自身を認証することが可能です。
- 管理者および信頼できるユーザーをデバイス管理グループに追加することで、[Device Access Manager]によるデバイスへのアクセス制限からこれらの管理者やユーザーを除外できます。このグループのメンバーシップは、[詳細設定]を使用して管理します。
- グループ メンバーシップに基づいて、または個々のユーザーに対して、デバイス アクセスを許可または拒否できます。
- CD-ROM ドライブや DVD ドライブなどのデバイス クラスの場合は、読み取りアクセスおよび書き込みアクセスを個別に許可または拒否できます。

Device Access Manager を開く

1. 管理者としてログオンします。
2. [**HP Client Security**]ダッシュボードから[**HP ProtectTools Security Manager**]を起動します。

   または

   Windows デスクトップで、タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンをダブルクリックします。

   または

   [**コントロール パネル**]→[**システムとセキュリティ**]→[**HP ProtectTools Security Manager**]の順に選択します。
3. HP ProtectTools Security Manager ユーザー コンソールの左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。
4. 管理者コンソールの左側の枠内で[**Device Access Manager**]をクリックします。

標準ユーザーは、HP ProtectTools Security Manager を使用して HP ProtectTools Device Access Manager ポリシーを表示できます。このコンソールのビューは読み取り専用です。

セットアップ手順

デバイス アクセスの設定

HP ProtectTools Device Access Manager には、以下の 4 つのビューがあります。

- [**簡易構成**]：デバイス管理者グループのメンバーシップに基づいて、デバイス クラスへのアクセスを許可または拒否します。
- [**デバイス クラス構成**]：特定のユーザーまたはグループに対して、特定の種類のデバイスまたは特定のデバイスへのアクセスを許可または拒否します。
- [**ジャスト イン タイム認証の構成**]：選択されたユーザーが自身を認証して DVD デバイスや CD-ROM デバイスまたはリムーバブル メディアにアクセスできるようにする、ジャスト イン タイム認証（JITA）を構成します。
- [**詳細設定**]：C ドライブ、システム ドライブなど、Device Access Manager によってアクセスを制限されないドライブ文字の一覧を構成します。デバイス管理者グループのメンバーシップもこのビューから管理できます。

簡易構成

管理者は、[**簡易構成**]ビューを使用して、デバイス管理者以外のすべてのユーザーによる以下のデバイス クラスへのアクセスを許可または拒否できます。

- すべてのリムーバブル メディア（フロッピーディスク、USB フラッシュ ドライブなど）
- すべての DVD/CD-ROM ドライブ
- すべてのシリアル ポートおよびパラレル ポート

- すべての Bluetooth デバイス

注記： Bluetooth デバイスを認証資格情報として使用する場合は、Device Access Manager ポリシーで Bluetooth デバイスへのアクセスを制限しないでください。

- すべてのモデム デバイス
- すべての PCMCIA/ExpressCard デバイス
- すべての 1394 デバイス

デバイス管理者以外のすべてのユーザーによるデバイス クラスへのアクセスを許可または拒否するには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールの左側の枠内で、［**Device Access Manager**］→［**簡易構成**］の順にクリックします。
2. アクセスを拒否するには、右側の枠内で、デバイス クラスまたは特定のデバイスのチェックボックスにチェックを入れます。アクセスを許可するには、デバイス クラスまたは特定のデバイスのチェックボックスのチェックを外します。

   チェック ボックスがグレーで表示されている場合は、アクセス方法に影響を与える値が［**デバイス クラス構成**］ビューで変更されています。工場出荷時の設定に戻すには、［**デバイス クラス構成**］ビューで［**リセット**］をクリックします。
3. ［**適用**］をクリックします。

   注記： バックグラウンド サービスが実行されていない場合は、サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。［**はい**］をクリックします。
4. ［**OK**］をクリックします。

バックグラウンド サービスの開始

新しいポリシーが初めて定義されて適用されると、[HP ProtectTools デバイス ロック/検査]バックグラウンド サービスが自動的に開始され、システムが起動するたびに自動的に開始するように設定されます。

注記： バックグラウンド サービスの開始を尋ねる画面が表示される前に、デバイス プロファイルを定義しておく必要があります。

管理者は、以下の操作を行うことでもサービスを開始または停止できます。

[HP ProtectTools デバイス ロック/検査]サービスを停止しても、デバイス ロックは停止されません。デバイス ロックは、以下の 2 つのコンポーネントによって実行されています。

- [HP ProtectTools デバイス ロック/検査]サービス
- DAMDrv.sys ドライバー

サービスを開始するとこのデバイス ドライバーが開始されますが、サービスを停止してもこのドライバーは停止されません。

このバックグラウンド サービスが実行されているかどうかを確認するには、コマンド プロンプト ウィンドウを開いて「`sc query flcdlock`」と入力します。

このデバイス ドライバーが実行されているかどうかを確認するには、コマンド プロンプト ウィンドウを開いて「`sc query damdrv`」と入力します。

デバイス クラス構成

管理者は、デバイス クラスまたは特定のデバイスへのアクセスを許可または拒否されているユーザーおよびグループを一覧から表示したり編集したりできます。

[**デバイス クラス構成**]ビューには以下のセクションがあります。

- [**デバイス一覧**]：デバイス クラス、およびシステムにインストールされているか以前にインストールされていた可能性のあるデバイスをすべて表示します。
  - 保護は、通常はデバイス クラスに対して適用されます。選択されたユーザーまたはグループは、そのデバイス クラスの任意のデバイスにアクセスできます。
  - 特定のデバイスに対して保護を適用することもできます。
- [**ユーザー一覧**]：選択されたデバイス クラスまたは特定のデバイスへのアクセスを許可または拒否されているユーザーおよびグループをすべて表示します。
  - [ユーザー一覧]には、特定のユーザーまたはそのユーザーがメンバーとなっているグループを登録できます。
  - [ユーザー一覧]でユーザーまたはグループを利用できない場合は、設定が[デバイス一覧]のデバイス クラスまたは[クラス]フォルダーから継承されています。
  - DVD や CD-ROM など一部のデバイス クラスでは、読み取りおよび書き込み操作のためのアクセスを個別に許可または拒否することによって詳細な制御を設定できます。

    それ以外のデバイスおよびクラスでは、読み取りおよび書き込みアクセス権を継承できます。たとえば、読み取りアクセス権は上位のクラスから継承し、書き込みアクセス権はユーザーまたはグループごとに定義するといった設定が可能です。

    注記： [**読み取り**]チェック ボックスのチェックが外れている場合、アクセス制御の登録内容はデバイスへの読み取りアクセスに影響を与えませんが、読み取りアクセスが拒否されるわけではありません。

    注記： Administrators グループを[ユーザー一覧]に追加することはできません。代わりに、デバイス管理者グループを使用します。

    例 1：ユーザーまたはグループがデバイスまたはデバイス クラスへの書き込みアクセスを拒否されている場合

    このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを許可できます。

    例 2：ユーザーまたはグループがデバイスまたはデバイス クラスへの書き込みアクセスを許可されている場合

    このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを拒否できます。

    例 3：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りアクセスを許可されている場合

    このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを許可できます。

例 4：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、読み取りアクセスまたは読み取りおよび書き込みアクセスを許可できます。

例 5：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りおよび書き込みアクセスを許可されている場合

このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを拒否できます。

例 6：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りおよび書き込みアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、読み取りアクセスまたは読み取りおよび書き込みアクセスを許可できます。

ユーザーまたはグループのアクセス拒否

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを拒否するには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールの左側の枠内で、［**Device Access Manager**］→［**デバイス クラス構成**］の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - ［**デバイス クラス**］
   - ［**すべてのデバイス**］
   - ［**個々のデバイス**］
3. ［**ユーザー/グループ**］で、アクセスを拒否するユーザーまたはグループを選択し、［**拒否**］をクリックします。
4. ［**適用**］をクリックします。

注記： 同じデバイス レベルでユーザーに対して拒否および許可を設定すると、アクセス許可よりもアクセス拒否が優先されます。

ユーザーまたはグループのアクセス許可

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを許可するには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールの左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスの一覧で、以下のどれかをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]
3. [**追加**]をクリックします。

   [**ユーザーまたはグループの選択**]ダイアログ ボックスが表示されます。
4. [**詳細**]をクリックし、[**今すぐ検索**]をクリックして、追加するユーザーまたはグループを検索します。
5. 使用可能なユーザーおよびグループの一覧に追加するユーザーまたはグループをクリックして[**OK**]をクリックします。
6. 再度[**OK**]をクリックします。
7. [**許可**]をクリックして、そのユーザーによるアクセスを許可します。
8. [**適用**]をクリックします。

グループの単一ユーザーによるデバイス クラスへのアクセス許可

デバイス クラスへのアクセスを、グループ内のある 1 人のユーザーだけに許可して、同じグループ内の他のメンバーには拒否するには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールの左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]
3. [**ユーザー/グループ**]で、アクセスを拒否するグループを選択し、[**拒否**]をクリックします。
4. 目的のクラスの下のフォルダーに移動して、特定のユーザーを追加します。
5. [**許可**]をクリックして、そのユーザーによるアクセスを許可します。
6. [**適用**]をクリックします。

グループの単一ユーザーによる特定のデバイスへのアクセス許可

管理者は、特定のデバイスへのアクセスを、グループ内のある 1 人のユーザーだけに許可して、同じグループ内の他のメンバーには拒否することができます。

1. HP ProtectTools 管理者コンソールの左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスのリストで、設定するデバイス クラスをクリックして、その下のフォルダーに移動します。
3. [**ユーザー/グループ**]で、アクセスを許可するグループの横にある[**許可**]をクリックします。
4. アクセスを拒否するグループの横にある[**拒否**]をクリックします。
5. デバイス リストで、ユーザーによるアクセスを許可する特定のデバイスに移動します。
6. [**追加**]をクリックします。

   [**ユーザーまたはグループの選択**]ダイアログ ボックスが表示されます。
7. [**詳細**]をクリックし、[**今すぐ検索**]をクリックして、追加するユーザーまたはグループを検索します。
8. アクセスを許可するユーザーをクリックして[**OK**]をクリックします。
9. [**許可**]をクリックして、そのユーザーによるアクセスを許可します。
10. [**適用**]をクリックします。

ユーザーまたはグループの設定削除

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを削除するには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールの左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]
3. [**ユーザー/グループ**]で、削除するユーザーまたはグループをクリックし、[**削除**]をクリックします。
4. [**適用**]をクリックします。

構成のリセット

注意： 構成をリセットすると、それまでに実行されたデバイスの構成変更がすべて破棄され、すべての設定が工場出荷時の設定値に戻ります。

注記： [詳細設定]ページはリセットされません。

構成設定を工場出荷時の値に戻すには、以下の操作を行います。

1. HP ProtectTools 管理者コンソールの左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. [**リセット**]をクリックします。
3. 確認要求に対して[**はい**]をクリックします。
4. [**適用**]をクリックします。

ジャスト イン タイム認証の構成

ジャスト イン タイム認証の構成では、管理者はジャスト イン タイム認証（JITA）を使用してデバイスへのアクセスを許可されるユーザーおよびグループの一覧を表示したり変更したりできます。

ジャスト イン タイム認証が有効なユーザーは、[**デバイス クラス構成**]または[**簡易構成**]ビューで作成されたポリシーが制限されている一部のデバイスにアクセスできます。

- シナリオ：[簡易構成]ポリシーは、DVD ドライブや CD-ROM ドライブへのデバイス管理者以外のアクセスをすべて拒否するように構成されています。
- 結果：ジャスト イン タイム認証が有効なユーザーが DVD ドライブや CD-ROM ドライブにアクセスしようとすると、ジャスト イン タイム認証が有効になっていないユーザーと同じ「アクセス拒否」メッセージが表示されます。次に、バルーン メッセージが表示され、ユーザーがジャスト イン タイム認証アクセスを希望するかどうかを尋ねます。バルーンをクリックすると、ユーザー認証ダイアログが表示されます。ユーザーが資格情報を正しく入力すると、DVD ドライブや CD-ROM ドライブへのアクセスが許可されます。

ジャスト イン タイム認証期間は、設定した時間（分）または 0 分の間有効です。ジャスト イン タイム認証期間を 0 分にすると、認証が有効のままになります。ユーザーは、認証されてからシステムからログオフするまで、デバイスにアクセスできます。

ジャスト イン タイム認証期間を延長するように構成することもできます。このシナリオでは、ジャスト イン タイム認証期間が失効する 1 分前に表示されるメッセージをクリックすることにより、再認証しなくてもアクセスを延長できるようにしています。

ユーザーに与えられるジャスト イン タイム認証期間が限定的か無制限かに関係なく、ユーザーがシステムをログオフしたり別のユーザーがログインしたりするとすぐに、ジャスト イン タイム認証期間は失効します。次にユーザーがログインし、ジャスト イン タイム認証が有効なデバイスにアクセスしようとすると、資格情報を入力するよう求めるメッセージが表示されます。

ジャスト イン タイム認証は以下のデバイス クラスに対して使用できます。

- DVD/CD-ROM ドライブ
- リムーバブル メディア

ユーザーまたはグループのジャスト イン タイム認証の作成

管理者は、ジャスト イン タイム認証を使用して、ユーザーまたはグループにデバイスへのアクセスを許可できます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。

3. [+]をクリックして、ユーザーまたはグループをジャスト イン タイム認証の構成に追加します。
4. [**有効**]チェック ボックスにチェックを入れます。
5. ジャスト イン タイム認証の期間を必要な時間に設定します。
6. [**適用**]をクリックします。

新しいジャスト イン タイム認証の設定を適用するには、ユーザーはログアウトしてからログオンしなおす必要があります。

ユーザーまたはグループの延長可能なジャスト イン タイム認証の作成

管理者は、ユーザーが失効前に延長できるジャスト イン タイム認証を使用して、ユーザーまたはグループにデバイスへのアクセスを許可できます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. [+]をクリックして、ユーザーまたはグループをジャスト イン タイム認証の構成に追加します。
4. [**有効**]チェック ボックスにチェックを入れます。
5. ジャスト イン タイム認証の期間を必要な時間に設定します。
6. [**延長可能**]チェック ボックスにチェックを入れます。
7. [**適用**]をクリックします。

新しいジャスト イン タイム認証の設定を適用するには、ユーザーはログアウトしてからログオンしなおす必要があります。

ユーザーまたはグループのジャスト イン タイム認証の無効化

管理者は、ジャスト イン タイム認証を使用して、ユーザーまたはグループによるデバイスへのアクセスを無効にできます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. ジャスト イン タイム認証を無効にするユーザーまたはグループを選択します。
4. [**有効**]チェック ボックスのチェックを外します。
5. [**適用**]をクリックします。

ユーザーがログインし、デバイスにアクセスしようとすると、アクセスは拒否されます。

詳細設定

[詳細設定]には以下の機能があります。

- デバイス管理者グループの管理
- Device Access Manager によって常にアクセスが許可されるドライブ文字の管理

デバイス管理者グループは、（デバイス アクセスに関して）信頼できるユーザーを Device Access Manager ポリシーによる制限から除外するために使用されます。信頼できるユーザーには、通常、システム管理者が含まれます。詳しくは、64 ページの「デバイス管理者グループ」を参照してください。

[**詳細設定**]ビューで、管理者は Device Access Manager がどのユーザーに対してもアクセスを制限しないドライブ文字の一覧を構成することもできます。

注記： ドライブ文字の一覧が構成されるときは Device Access Manager のバックグラウンド サービスが実行されている必要があります。

これらのサービスを開始するには、以下の操作を行います。

1. リムーバブル メディアへのデバイス管理者以外のアクセスを拒否するなど、簡易構成ポリシーを適用します。

   または

   管理者権限でコマンド プロンプト ウィンドウを開き、以下のように入力します。

   ```
   sc start flcdlock
   ```

   enter キーを押します。

2. サービスが開始されると、ドライブ一覧を編集できるようになります。Device Access Manager で制御しないデバイスのドライブ文字を入力します。

   物理的なハード ディスクまたはパーティションのドライブ文字が表示されます。

   注記： システム ドライブ（通常は C）がこの一覧に含まれているかどうかに関係なく、システム ドライブへのアクセスはどのユーザーに対しても拒否されません。

デバイス管理者グループ

Device Access Manager をインストールすると、デバイス管理者グループが作成されます。

デバイス管理者グループは、（デバイス アクセスに関して）信頼できるユーザーを Device Access Manager ポリシーによる制限から除外するために使用されます。信頼できるユーザーには、通常、システム管理者が含まれます。

注記： ユーザーをデバイス管理者に追加しても、そのユーザーによるデバイスへのアクセスが自動的に許可されるわけではありません。[**デバイス クラス構成**]ビューで、Users グループがデバイスへのアクセスを拒否されている場合、デバイス管理者グループのメンバーがデバイスにアクセスできるようにするには、デバイス管理者グループによるアクセスが許可されている必要があります。ただし、[**簡易構成**]ビューを使用して、デバイス管理者グループのメンバーではないすべてのユーザーによるデバイス クラスへのアクセスを拒否できます。

ユーザーをデバイス管理者グループに追加するには、以下の操作を行います。

1. [**詳細設定**]ビューで、[+]をクリックします。
2. 信頼できるユーザーのユーザー名を入力します。
3. [**OK**]をクリックします。
4. [**適用**]をクリックします。

eSATA デバイスのサポート

Device Access Manager で eSATA デバイスを制御するには、以下を構成する必要があります。

1. システムの起動時にドライブが接続されている必要があります。
2. [**詳細設定**]ビューを使用して、Device Access Manager がアクセスを拒否しないドライブの一覧に eSATA ドライブ文字が含まれていないことを確認します。eSATA ドライブ文字が一覧に含まれている場合は、ドライブ文字を削除して[**適用**]をクリックします。
3. デバイスは、[**簡易構成**]ビューまたは[**デバイス クラス構成**]ビューで[リムーバブル メディア] デバイス クラスを使用して制御できます。

管理されないデバイス クラス

HP ProtectTools Device Access Manager では、以下のデバイス クラスは管理されません。

- 入出力デバイス
  - バイオメトリック（生体認証）
  - マウス
  - キーボード
  - プリンター
  - プラグ アンド プレイ（PnP）プリンター
  - プリンター アップグレード
  - 赤外線ヒューマン インターフェイス デバイス
  - スマート カード リーダー
  - マルチポート シリアル
  - ディスク ドライブ
  - フロッピー ディスク コントローラー（FDC）

- ハード ディスク コントローラー（HDC）
- ヒューマン インターフェイス デバイス（HID）クラス
- 電源
  - バッテリ
  - Advanced Power Management（APM）サポート
- その他
  - コンピューター
  - デコーダー
  - ディスプレイ
  - プロセッサ
  - システム
  - 不明
  - ボリューム
  - ボリューム スナップショット
  - セキュリティ デバイス
  - セキュリティ アクセラレーター
  - Intel®統合ディスプレイ ドライバー
  - メディア ドライバー
  - メディア チェンジャー
  - 多機能
  - Legacard
  - ネット クライアント
  - ネット サービス
  - ネット転送
  - SCSI アダプター

8 盗難からの回復（一部のモデルのみ）

Computrace for HP ProtectTools（別売）を使用すると、コンピューターをリモートで監視、管理、および追跡できます。

Computrace for HP ProtectTools を有効にすると、Absolute Software Customer Center からツールの設定が行われます。管理者は Customer Center から Computrace for HP ProtectTools を設定し、コンピューターを監視または管理できます。システムの置き忘れや盗難が発生した場合、Customer Center はコンピューターを探索し取り戻すために地域当局に協力します。設定によって、ハードドライブが消去または交換された場合でも Computrace が動作し続けるようにすることができます。

Computrace for HP ProtectTools を有効にするには、以下の操作を行います。

1. インターネットに接続します。
2. HP ProtectTools Security Manager ユーザー コンソールを開きます。詳しくは、28 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
3. [HP ProtectTools Security Manager]の左側の枠内で[**盗難からの回復**]をクリックします。
4. Computrace 有効化ウィザードを起動するには、[**開始**]をクリックします。
5. 連絡先情報とクレジット カードの支払い情報を入力するか、または事前に購入したプロダクト キーを入力します。

[有効化ウィザード]によって取引が安全に処理され、Absolute Software カスタマー センターの Web サイトにユーザー アカウントがセットアップされます。完了すると、カスタマー センターのアカウント情報を含む確認の電子メールが届きます。

以前に Computrace 有効化ウィザードを実行したことがあり、Customer Center ユーザー アカウントをすでに持っている場合は、サポート窓口に問い合わせて追加ライセンスを購入できます。

カスタマー センターにログオンするには、以下の操作を行います。

1. https://cc.absolute.com/ （英語サイト）にアクセスして、ドロップダウン リストから[**日本語**]を選択します。
2. [**ユーザー名**]フィールドおよび[**パスワード**]フィールドに、確認の電子メールで受信した資格情報を入力し、[**ログイン**]をクリックします。

カスタマー センターでは、以下の操作を実行できます。

- コンピューターの監視
- リモート データの保護
- Computrace で保護されているコンピューターの盗難の報告

▲ Computrace for HP ProtectTools について詳しくは、[**詳細情報**]をクリックしてください。

9 ローカライズされたパスワードの例外事項

ブート前セキュリティ レベルおよび HP Drive Encryption レベルでは、以下の項目で説明しているように、パスワードのローカライズのサポートに制限があります。

パスワードが拒否された場合の対処方法

パスワードは、以下の原因で拒否されることがあります。

- サポートされていない IME をユーザーが使用している場合。これは、2 バイト文字言語（韓国語、日本語、中国語）ではよく起こる問題です。この問題を解決するには、以下の操作を行います。

  1. [**コントロール パネル**] を使用して、サポートされているキーボード レイアウトを追加します（[入力言語]の[中国語]の下で、[US/英語]キーボードを追加します）。
  2. サポートされているキーボードを初期の入力言語に設定します。
  3. HP ProtectTools を再起動してから、パスワードを再度入力します。

- ユーザーがサポートされていない文字を使用している場合。この問題を解決するには、以下の操作を行います。

  1. サポートされている文字のみを使用するように Windows パスワードを変更します。サポートされていない文字について詳しくは、HP ProtectTools 管理者コンソール ソフトウェアのヘルプを参照してください。
  2. HP ProtectTools Security Manager セットアップ ウィザードを実行しなおし、新しい Windows パスワードを入力します。

Windows IME はブート前セキュリティ レベルまたは HP Drive Encryption レベルではサポートされない

Windows では、IME（Input Method Editor：入力方式エディター）を選択することによって、日本語や中国語の文字などの複雑な文字および記号を、一般的な西洋言語用のキーボードを使用して入力できます。

IME は、ブート前セキュリティ レベルまたは HP Drive Encryption レベルではサポートされていません。ブート前セキュリティまたは HP Drive Encryption のログイン画面では、IME を使用して Windows パスワードを入力することはできません。また、入力しようとすると、ロックアウトが発生することがあります。場合によっては、パスワードの入力時に Microsoft Windows によって IME が表示されないこともあります。

この問題を解決するには、サポートされている以下のどれかのキーボード レイアウトに切り替えます。これらのキーボード レイアウトは、キーボード レイアウト 00000411 に変換されます。

- 日本語 Microsoft IME
- 日本語キーボード レイアウト
- Office 2007 IME（日本語）：Microsoft や他社が、IME または入力方式エディターという用語を使用していても、その入力方式が実際には IME ではない場合があります。このため、混乱が生じることもありますが、ソフトウェアは 16 進表記を読み取ります。したがって、サポートされているキーボード レイアウトに IME がマッピングされている場合、HP ProtectTools はその設定をサポートできます。

警告！ HP ProtectTools を使用すると、Windows IME を使用して入力したパスワードは拒否されます。

サポートされている別のキーボード レイアウトを使用したパスワードの変更

初期パスワードをあるキーボード レイアウト（たとえば、英語（米国）（409））を使用して設定し、後から、サポートされている別のキーボード レイアウト（たとえば、ラテン アメリカ言語（080A））を使用して変更すると、そのパスワードの変更は HP Drive Encryption では正常に認識されます。ただし、ラテン アメリカ言語に存在して、英語（米国）には存在しない文字（たとえば、ē）を使用すると、BIOS では正常に認識されません。

注記： 管理者はこの問題を解決できます。[HP ProtectTools ユーザーの管理]機能を使用して、HP ProtectTools からこのユーザーを削除し、オペレーティング システムで目的のキーボード レイアウトを選択してから、同じユーザーに対して Security Manager セットアップ ウィザードを実行しなおします。BIOS に目的のキーボード レイアウトが保存され、このキーボード レイアウトを使用して入力できるパスワードが BIOS 内に適切に設定されます。

もう 1 つ問題になる可能性があるのが、同じ文字を出力できる、異なるキーボード レイアウトを使用している場合です。たとえば、米国インターナショナル キーボード レイアウト（20409）とラテン アメリカ言語キーボード レイアウト（080A）は、どちらも文字 é を出力できますが、異なる順序でキーを操作しなければならないことがあります。最初にラテン アメリカ言語キーボード レイアウトを使用してパスワードを設定すると、その後に米国インターナショナル キーボード レイアウトを使用してパスワードを変更しても、BIOS にはラテン アメリカ言語キーボード レイアウトが設定されます。

特別なキーの扱い

- 中国語、スロバキア語、カナダ フランス語、およびチェコ語

  上記のキーボード レイアウトのどれかを選択してパスワードを入力した場合（たとえば、abcdef）、BIOS ブート前セキュリティおよび HP Drive Encryption では、同じパスワードを小文字の場合は shift キーを押しながら、大文字の場合は shift キーと caps lock キーを押しながら入力する必要があります。数字のパスワードは、テンキーを使用して入力する必要があります。

- 韓国語

  サポートされている韓国語キーボード レイアウトを選択してパスワードを入力した場合、BIOS ブート前セキュリティおよび HP Drive Encryption では、同じパスワードを小文字の場合は右 alt キーを押しながら、大文字の場合は右 alt キーと caps lock キーを押しながら入力する必要があります。

- サポートされていない文字は、以下の表のとおりです。

言語	Windows	BIOS	Drive Encryption
アラビア語	ﻹ、ﻵ、およびﻷキーは、2 文字になります	ﻹ、ﻵ、およびﻷキーは、1 文字になります	ﻹ、ﻵ、およびﻷキーは、1 文字になります
カナダ フランス語	caps lock を押した状態で入力した ç、è、à、および é は、Windows では Ç、È、À、および É になります	caps lock を押した状態で入力した ç、è、à、および é は、BIOS ブート前セキュリティでは ç、è、à、および é になります	caps lock を押した状態で入力した ç、è、à、および é は、HP Drive Encryption では ç、è、à、および é になります
スペイン語	40a はサポートされていません。ただし、ソフトウェアによって c0a に変換されるため、40a は正常に動作します。しかし、これらのキーボード レイアウトはわずかに異なるため、スペイン語を話すユーザーは、Windows のキーボード レイアウトを 1040a（スペイン語（バリエーション））または 080a（ラテン アメリカ言語）に変更することをおすすめします	n/a	n/a
米国インターナショナル	◦ 1 番上の行にある¡、¤、‘,’、¥、および×キーは拒否されます ◦ 1 番上の行にある å、®、および Þ キーは拒否されます ◦ 1 番上の行にある á、ð、および ø キーは拒否されます ◦ 1 番下の行にある æ キーは拒否されます	n/a	n/a

言語	Windows	BIOS	Drive Encryption
チェコ語	◦ ğ キーは拒否されます ◦ į キーは拒否されます ◦ ų キーは拒否されます ◦ ė、ı、および ż キーは拒否されます ◦ ģ、ķ、ļ、ņ、および ŗ キーは拒否されます	n/a	n/a
スロバキア語	ż キーは拒否されます	◦ š、ś、および ş キーは、入力した場合は拒否されますが、ソフト キーボードを使用して入力した場合は受け入れられます ◦ ţ デッド キーは 2 文字になります	n/a
ハンガリー語	ż キーは拒否されます	ţ キーは 2 文字になります	n/a
スロベニア語	żŻ キーは Windows では拒否されます。また、alt キーは、BIOS ではデッド キーとなります	ú、Ú、ů、Ů、ş、Ş、ś、Ś、š、および Š キーは、BIOS では拒否されます	n/a
日本語	利用できる場合は、Microsoft Office 2007 IME を選択することをおすすめします。IME という名前は付いていますが、実際にはキーボード レイアウト 411 であり、サポートされています	n/a	n/a

用語集

Drive Encryption
ハードドライブを暗号化して､適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護します。

Drive Encryption のログオン画面
Windows が起動する前に表示されるログオン画面。ユーザーは、Windows のユーザー名およびパスワード、またはスマート カード PIN を入力する必要があります。ほとんどの場合、Drive Encryption のログオン画面で正しい情報を入力すれば、Windows のログオン画面で再度ログオンすることなく、直接 Windows にアクセスできます。

DriveLock
ハードドライブをユーザーにリンクして､コンピューターの起動時にユーザーに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

HP SpareKey のリカバリ
セキュリティに関する質問に正しく回答することでコンピューターにアクセスできる機能。

ID
HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）内で、特定のユーザーのアカウントまたはプロファイルのように処理される、資格情報と設定の集合。

ID カード
ユーザー名および選択された画像を使用してデスクトップを視覚的に識別するための、Windows デスクトップのガジェット。

JITA
ジャスト イン タイム認証。

PIN
個人識別番号。

PKI
資格情報および暗号化キーを作成、使用、および管理するためのインターフェイスを定義する、公開キー基盤の規格。

SATA device mode（SATA デバイス モード）
コンピューターと大容量ストレージ デバイス（ハードドライブやオプティカル ドライブなど）の間のデータ転送モード。

Trusted Platform Module（トラステッド プラットフォーム モジュール）内蔵セキュリティ チップ
HP ProtectTools Embedded Security チップの一般的な呼び方。TPM では､ホスト システムに固有の情報（暗号化キー、デジタル署名、パスワードなど）が格納され、ユーザーではなくコンピューターが認証されます。TPM を使用すると、物理的な盗難や外部のハッカーによる攻撃によってコンピューター上の情報が危険にさらされるリスクを最小限に抑えることができます。

TXT
Trusted Execution Technology（トラステッド エグゼキューション テクノロジ）の略。

Windows 管理者
アクセス権を変更し、他のユーザーを管理するすべての権限を持つユーザー。

Windows ユーザー アカウント
ネットワークまたは個別のコンピューターへのログオンを承認された個人のプロファイル。

Windows ログオンのセキュリティ
アクセスのために特定の資格情報を使用するよう求めることで、Windows アカウントを保護できます。

暗号化
権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号化サービス プロバイダー（CSP）
明確なインターフェイスを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除
暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）
選択されたフォルダー内のすべてのファイルおよびサブフォルダーを暗号化するシステム。

暗号法
特定の個人のみが解読できるように、データを暗号化および暗号化解除する手法。

管理者
「Windows 管理者」を参照してください。

管理者コンソール
管理者が HP ProtectTools の機能および設定に対するアクセスや管理を行うことができる、中心となる場所。

緊急リカバリ アーカイブ
他のプラットフォームの所有者キーを使用して基本ユーザー キーを再暗号化できる、保護された記憶領域。

グループ
デバイス クラスまたは特定のデバイスに対して同じレベルのアクセス許可またはアクセス拒否が設定されているユーザーのグループ。

シーン
登録されたユーザーの認証に使用する画像。

資格情報
ユーザーが認証プロセスで特定のタスクに対する適格性を証明するための手段。

指紋
指紋の画像をデジタルの形式で抽出したもの。実際の指紋の画像は、HP ProtectTools Security Manager には保存されません。

シングルサインオン
認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに HP ProtectTools Security Manager を使用してアクセスできるようにする機能。

スマート カード

所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピューターに対して認証するために使用されます。

セキュリティ ログオン方法
コンピューターへのログオンに使用される方法。

デバイス アクセス制御ポリシー
ユーザーがアクセスを許可または拒否されているデバイスの一覧。

デバイス クラス
ドライブなど、特定の種類にあてはまるすべてのデバイス。

電源投入時認証
スマート カード、セキュリティ チップ、パスワードなど、コンピューターの起動時に何らかの形式の認証を要求するセキュリティ機能。

ドメイン
ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピューターの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

認証
ユーザーがタスクの実行（コンピューターへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

認証機関（CA）
公開キー基盤の運営に必要な証明書を発行するサービス。

ネットワーク アカウント
ローカル コンピューター上、ワークグループ内、またはドメイン上の Windows ユーザーまたは管理者のアカウント。

バイオメトリック（生体認証）
指紋などの身体的な特徴を使用してユーザーを識別する認証証明のカテゴリ。

廃止パスワード
ユーザーがデジタル証明書を要求するときに作成されるパスワード。このパスワードは、ユーザーがデジタル証明書を廃止する場合に必要です。これによって、ユーザー自身のみが証明書を廃止できるようになります。

バックアップ
バックアップ機能を使用して、重要なプログラム情報のコピーをそのプログラムの外部の場所に保存すること。バックアップした内容は、後日、同じコンピューターまたは別のコンピューターに情報を復元するために使用できます。

バックグラウンド サービス
デバイス アクセス制御ポリシーを適用するには、[HP ProtectTools デバイス ロック/検査]バックグラウンド サービスが実行されている必要があります。このサービスは、[コントロール パネル]の[管理ツール]オプションにある[サービス]アプリケーションで確認できます。このサービスが実行されていない場合、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）は、デバイス アクセス制御ポリシーが適用されているときにサービスを起動しようと試みます。

フォルダー/ファイル
個人の情報やファイル、履歴や Web 関連のデータなどを含むデータ コンポーネントのことで、ハードドライブ上に存在します。

復元
以前に保存されたバックアップ ファイルから、プログラム情報をこのプログラムにコピーするプロセス。

有効化

Drive Encryption の機能にアクセスする前に完了する必要があるタスク。Drive Encryption は、HP ProtectTools セットアップ ウィザードを使用して有効にします。管理者のみが Drive Encryption を有効にできます。有効化プロセスは、ソフトウェアの有効化、ドライブの暗号化、ユーザー アカウントの作成、およびリムーバブル ストレージ デバイス上の初期バックアップ暗号化キーの作成で構成されます。

ユーザー
Drive Encryption に登録された人。管理者以外のユーザーは、Drive Encryption での権限が制限されています。管理者以外のユーザーが実行できる操作は、登録（管理者の許可がある場合）とログオンのみです。

リブート
コンピューターを再起動するプロセス。

ログオン
Web サイトやその他のプログラムにログオンするために使用できるユーザー名とパスワード（またはその他の選択された情報）で構成される、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）内のオブジェクト。

索引